{'type': 'Image', 'element\_id': 'a70395f744d215223f9ee4cef405746e', 'text': '24 SECURING 5G and EVOLVING ARCHITECTURES PRAMOD NAIR = /O\_\\TFE\\)B', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 1, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3c983550e285090b4a42ed8a5a25ce92', 'text': 'Securing 5G and Evolving Architectures', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 2, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2cf50d9867af81253467676403501ab7', 'text': 'Pramod Nair', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 2, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f4cc732268366a62870c65929ea00350', 'text': 'vvAddison-Wesley', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 2, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c51a98bae11cc52e980ecd7b52dc8207', 'text': 'Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 3, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e826f8c2cb49f09e6a51c0252d662c7e', 'text': 'The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 3, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f434aff83943337d988a8ff0e62cec20', 'text': 'For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 3, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '70a7b15a17b1bfef3b4a6ef814781d42', 'text': 'For government sales inquiries, please contact', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 3, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '51518b625f70fa2519d14dc8601f0dab', 'text': 'For government sales inquiries, please contact governmentsales@pearsoned.com.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 3, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '387758b8658df711f2a413b0305d00ce', 'text': 'For questions about sales outside the U.S., please contact intlcs@pearson.com.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 3, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0a268ab0ffad818e3cef9785d9df4642', 'text': 'Visit us on the Web: informit.com/aw', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 3, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b816e18c1f0f7fc76d2cc6da93da7e0b', 'text': '[PE: Copy the LOC Control Number line from the email.]', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 3, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6de56c7c3342397bffaa5f5017327b5d', 'text': 'Library of Congress Control Number: 2021917555', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 3, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '002b82034f0c3f82b55e57d039117eed', 'text': 'Copyright © 2022 Pearson Education, Inc.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 3, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5580a58544289355e343f4a93a23946e', 'text': 'All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 3, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2587e6e76faaef24bb7862a9625b84d7', 'text': 'No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 3, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4c6e2c95fb837a302efeb0e83423b93d', 'text': 'for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '031371a5df143483216d9d21d4260f6d', 'text': 'ISBN-13: 978-0-13-745793-9', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f2e0efc9174128d0528b7614affe6ae5', 'text': 'ISBN-10: 0-13-745793-6', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a22a46925548377f2aa78709cf10c8b2', 'text': 'ScoutAutomatedPrintCode', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '42cdbfb5f400cb75991bcd2d7731efa3', 'text': 'Editor-in-Chief', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0c3bb0ab245c05bfa32b920ae5e03d35', 'text': 'Mark Taub', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fb06a284116bb57883035731d81d8e5a', 'text': 'Product Line Manager', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9210260ed93d552a0748315d5e59f727', 'text': 'Brett Bartow', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd9543fdb40eb9b6a49f22541747d8b33', 'text': 'Executive Editor', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c943ae9b94923e84afd6cf992a643488', 'text': 'Nancy Davis', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aad81e83aa373262450fbd149b841e13', 'text': 'Development Editor', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a8dc9032f1c8ad8059f9c0d9edd087a4', 'text': 'Christopher A. Cleveland', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '59cb9e4f55b35a502d32a54d0241fb0e', 'text': 'Managing Editor', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '642fbd2c66aae56881e7964055fd73ea', 'text': 'Sandra Schroeder', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '74eef291f26d7682bda0e10948520117', 'text': 'Project Editor', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '500f74d541d54b7710fe3d77d75a9f5c', 'text': 'Mandie Frank', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '02087b7cb2f08f7bf3d0baedcdfed282', 'text': 'Copy Editor', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e8f1cdbdf721603262db9d520da3be34', 'text': 'Bart Reed', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da0634531377edf401c6af0ef1e27727', 'text': 'Indexer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3eae94923e4d81eead111e55ce49c284', 'text': 'Proofreader', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f182e9da37a5fc68908d5605ea90dbfd', 'text': 'Technical Reviewers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a8ce9b19c43f8a15a1e233240643fbb9', 'text': 'Dave Hucaby', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c1b9d115cf8a249bb28575b893a1aa5b', 'text': 'Keith O’Brien', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b28465c43a79306b5ed483ab8ff52a2f', 'text': 'Editorial Assistant', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0df66945ca4e2c1383a56d28a292648f', 'text': 'Cindy Teeters', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1634dd44ab6e0ae40775442394c57b57', 'text': 'Designer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6862ff37b1c372d1cdc93ae8d75acdf6', 'text': 'Chuti Prasertsith', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 4, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'be754ea7267f6667de529daa8b6584f0', 'text': 'Compositor', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 5, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '43193efd6576860a83d9f98a1d431da7', 'text': 'codeMantra', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 5, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2606966d31b67e8bcce33991aa22e461', 'text': 'Graphics', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 5, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '21889f95cb5321cda80352e0d126c0b0', 'text': 'codeMantra', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 5, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67992ca039facdbab4dae6140db76a33', 'text': 'I would like to dedicate this book to my family. Thank you for the unwavering support, motivation and patience throughout the development of this book.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 6, 'parent\_id': '3c983550e285090b4a42ed8a5a25ce92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6bf4bb3e2dbaa983d78bd62e43236e98', 'text': 'Contents', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7daf76bb38334beb54ae937557e46145', 'text': 'Part I: Evolution of Cellular Technologies to 5G: Security Enhancements and Challenges', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58e71a1d5b2bc8df7ad159fb5bc6abba', 'text': 'Chapter 1. Evolution from 4G to 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '7daf76bb38334beb54ae937557e46145', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bb7a95deaaa9939a7266c6bb265e93d0', 'text': 'Chapter 2. Deployment Modes in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '7daf76bb38334beb54ae937557e46145', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '43d719b726df203864cb7d4aa20952c9', 'text': 'Chapter 3. Securing 5G Infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '7daf76bb38334beb54ae937557e46145', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '76df5d24f5201addb0005228f3f1b177', 'text': 'Part II: Securing 5G Architectures, Deployment Modes, and Use Cases”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '933101782b5da14c3a93d44216f566f2', 'text': 'Chapter 4. Securing RAN and Transport Deployments in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '76df5d24f5201addb0005228f3f1b177', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '579a842139164990a687b7118ed3cd69', 'text': 'Chapter 5. Securing MEC Deployments in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '76df5d24f5201addb0005228f3f1b177', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6faa413f73d8b1af773c76a848107ab8', 'text': 'Chapter 6. Securing Virtualized 5G Core Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '76df5d24f5201addb0005228f3f1b177', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0deebdb243376d8a607513725c30f2a1', 'text': 'Chapter 7. Securing Network Slice, SDN, and Orchestration in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '76df5d24f5201addb0005228f3f1b177', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0013238f7847af50768ae59ab378e6c2', 'text': 'Chapter 8. Securing Massive IoT Deployments in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '76df5d24f5201addb0005228f3f1b177', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '04583ef6296e1c7bcd05a0afc8421c9c', 'text': 'Chapter 9. Securing 5G Use Cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '76df5d24f5201addb0005228f3f1b177', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f7e272c17a843c7b1918893858bd00eb', 'text': 'Part III: End to End 5G Security Architecture and Prioritizing Security Investments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '76df5d24f5201addb0005228f3f1b177', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c7618b27c6b175e06056a33cf9790db5', 'text': 'Chapter 10. Building Pragmatic End-to-End 5G Security Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '76df5d24f5201addb0005228f3f1b177', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a0611431ee20c2f853bb8aa39572c59e', 'text': 'Chapter 11. Prioritizing 5G Security Investments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '76df5d24f5201addb0005228f3f1b177', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed0e8e068cc5d32db23972540a592daa', 'text': 'Part IV: Emerging Discussions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '76df5d24f5201addb0005228f3f1b177', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd0375504784a0b56211e26d16ede6182', 'text': 'Chapter 12. 5G and Beyond', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 7, 'parent\_id': '76df5d24f5201addb0005228f3f1b177', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f0bce6a1eb3c78252a9322f6d6a4e906', 'text': 'Table of Contents', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a93771a086d308dd8690ba8799981c79', 'text': 'Part I: Evolution of Cellular Technologies to 5G: Security Enhancements and Challenges', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '78e070ab19863b0ee91fffe68489c120', 'text': 'Chapter 1. Evolution from 4G to 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '68384fa10c3b7ee7d0d899a254a60b90', 'text': 'Mobile Network Evolution from 4G to 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '35cfdce2f583176f638ddbcdc255de19', 'text': '5G New Radio Features', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '49e10af94f2feb8cb51ee0bbde9882b8', 'text': 'Disaggregated Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0b9ea508d336849277ce8c41839128bb', 'text': 'Key 5G Features in 3GPP Releases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8f757445913210f8b0f28485eebb051b', 'text': 'Key 5G Advanced Features', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ea48edf62a0913aa4aad3a46860fec06', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '77b70f33cc26adceae2b761bf8700951', 'text': 'Acronym Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3230457333631936c21a38ff23919570', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e7c4fa50296c78ba288712d3bf8a4bd9', 'text': 'Chapter 2. Deployment Modes in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd2c31ed3b9f093cf9dd587284e5a083f', 'text': '5G NSA and SA Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1a41fe57f7d3c0623c36d843079f999f', 'text': '5G Time-Sensitive Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e2a6866524d3c39faf17cf2de944c144', 'text': '5G Local Area Network–Type Service', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6ab6e326273d45082c5d74258c5ba85a', 'text': 'Private 5G/Non-Public Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4363cbe63263c6ddf210c416a40d3dcc', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d40bbe9d5e477afc5736732616024e2', 'text': 'Acronym Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '66c4a4019960c22b3eb00991e2aaa8a7', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd8efb0366f917416a9e454dda6be3ac0', 'text': 'Chapter 3. Securing 5G Infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8bbca2533fc0234378c0e28c44260872', 'text': '3GPP 5G Security Enhancements', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67db0cfbeea133b42f2d377a9cca3448', 'text': 'Security Challenges in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8c7294645efc46f5e383638402bba4f1', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 8, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '81935d1f7533739533afff97b3a6650f', 'text': 'Acronyms Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bdae9387e51f42d0d4d4628136a04877', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': 'a93771a086d308dd8690ba8799981c79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a3376ff9f67cf9c9a5d6054ddda34267', 'text': 'Part II: Securing 5G Architectures, Deployment Modes, and Use Cases”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2b85fa6d1bd9b20328985eca5bfb734c', 'text': 'Chapter 4. Securing RAN and Transport Deployments in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': 'a3376ff9f67cf9c9a5d6054ddda34267', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6c1ff207c7017a3bc81e4b6ab6130206', 'text': '5G RAN and Transport Threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': 'a3376ff9f67cf9c9a5d6054ddda34267', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7ef13a0f0eca78fd3b4994aa5b21d9dd', 'text': 'Securing 5G RAN and Transport', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': 'a3376ff9f67cf9c9a5d6054ddda34267', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f6563004069cf3a8e3fa1b9344f9e804', 'text': 'Real Scenario Case Study: Examples of Threat Surfaces and Their Mitigation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': 'a3376ff9f67cf9c9a5d6054ddda34267', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '97b695117eb9850aba700e835c537302', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': 'a3376ff9f67cf9c9a5d6054ddda34267', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8526bd0ee84f1d26bda4a428101d4e16', 'text': 'Acronym Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': 'a3376ff9f67cf9c9a5d6054ddda34267', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bbcc00c47647c16d7843be6d4326cef8', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': 'a3376ff9f67cf9c9a5d6054ddda34267', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '72cc65706af62b054943786d8d77c6e5', 'text': 'Chapter 5. Securing MEC Deployments in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ff88119cc2c4c4f01c2ceb3bede735c5', 'text': 'Service Provider Network-Based MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': '72cc65706af62b054943786d8d77c6e5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bf69bebe7ae80fca737fb7d653c38774', 'text': 'Enterprise Network-Based MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': '72cc65706af62b054943786d8d77c6e5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd1c9192f4a5cebb73f6deed045a5891c', 'text': 'MEC Deployment Models', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': '72cc65706af62b054943786d8d77c6e5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '003ff634f8b897a8defd803780239ff4', 'text': 'Threat Surfaces in 5G MEC Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': '72cc65706af62b054943786d8d77c6e5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c0cb3c4275ffd2e695688dbaa92033fd', 'text': 'Securing 5G MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': '72cc65706af62b054943786d8d77c6e5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '30284fdee434710dcb72f4d1abd1d6cc', 'text': 'Real Scenario Case Study: MEC Threats and Their Mitigation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': '72cc65706af62b054943786d8d77c6e5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e392de1b309f2a93a8d24f30f7dffbb3', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': '72cc65706af62b054943786d8d77c6e5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4afde3e9c8686be21dfbcfab14791f30', 'text': 'Acronym Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': '72cc65706af62b054943786d8d77c6e5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd2ed6f680e74573ccfb672d17a4d9cdb', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': '72cc65706af62b054943786d8d77c6e5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a27046046a07e01bcdebf8db7a74cbc5', 'text': 'Chapter 6. Securing Virtualized 5G Core Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e2064fe7ed4a9706dcf16bf3f90d0b94', 'text': 'A Brief Evolution of Virtualization in Telecommunications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': 'a27046046a07e01bcdebf8db7a74cbc5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a32cdc8e2236178531a46f71e4939214', 'text': 'Threats in Virtualized 5G Packet Core Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': 'a27046046a07e01bcdebf8db7a74cbc5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9873c1cf443a535bdaf9c857c62f92cc', 'text': 'Securing Virtualized 5G Packet Core Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': 'a27046046a07e01bcdebf8db7a74cbc5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3bb372f910c4d16bc436d0575ff9c9c4', 'text': 'Real Scenario Case Study: Virtualized 5GC Threats and Mitigation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 9, 'parent\_id': 'a27046046a07e01bcdebf8db7a74cbc5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e1d19fbb1678446926fb8786d30ad91', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'a27046046a07e01bcdebf8db7a74cbc5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '11f6a966f5b3805e8ed04ad6ad8a6f33', 'text': 'Acronym Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'a27046046a07e01bcdebf8db7a74cbc5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bd0a13f96ff5f3259e71a2cc709fa493', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'a27046046a07e01bcdebf8db7a74cbc5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c6f0e84f72640c8754993ca4c5257af1', 'text': 'Chapter 7. Securing Network Slice, SDN, and Orchestration in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e33a83d1a0105495ccb48b6b80d95a09', 'text': 'Network Slicing and Its Enablers—SDN and Orchestration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'c6f0e84f72640c8754993ca4c5257af1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '278e2cdbda289831f1532d806cfe0fb5', 'text': 'Threat Surfaces in 5G Network Slice, SDN, and Orchestration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'c6f0e84f72640c8754993ca4c5257af1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2aff1c3b11f6a810f2c3c07071c78c72', 'text': 'Threat Surfaces in 5G Network Slice, SDN, and Orchestration Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'c6f0e84f72640c8754993ca4c5257af1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd6cb3a729d0e5843b40d7d53ccc25681', 'text': 'Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'c6f0e84f72640c8754993ca4c5257af1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5f59480b199ec98c6e307a6eeb4361fd', 'text': 'Mitigation of Threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'c6f0e84f72640c8754993ca4c5257af1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3875dcedad0208804f452edd21f29dc7', 'text': 'Real Scenario Case Study: Threats in the 5G Network Slice, SDN, and Orchestration Deployments and Their Mitigation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'c6f0e84f72640c8754993ca4c5257af1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '19769db8beddd61c2d5e0d404f757200', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'c6f0e84f72640c8754993ca4c5257af1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '93593ff933ae109a351f03f2f6fd8e11', 'text': 'Key Acronyms', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'c6f0e84f72640c8754993ca4c5257af1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '090c7263e05ce688835b3c2a7cdedd70', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'c6f0e84f72640c8754993ca4c5257af1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f44a9497d3681ac824b379235c34b917', 'text': 'Chapter 8. Securing Massive IoT Deployments in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a0f8558cedc9d3d678422e515fcd773', 'text': 'Massive IoT–Based Threats in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'f44a9497d3681ac824b379235c34b917', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '95108e2c4c1233bab8934fbb0f9aedd4', 'text': 'Securing mIoT Deployments in 5G Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'f44a9497d3681ac824b379235c34b917', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '29d0c19bc37347675805a74cc8b65200', 'text': 'Real Scenario Case Study: mIoT Threats and Their Mitigation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'f44a9497d3681ac824b379235c34b917', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '77d039d194bfdb484362bfebe92f2206', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'f44a9497d3681ac824b379235c34b917', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ce3418c7b70c794a8784a15564b61968', 'text': 'Key Acronyms', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'f44a9497d3681ac824b379235c34b917', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ae0a2e361add9c95cf9c8018a33a4984', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': 'f44a9497d3681ac824b379235c34b917', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '693b38087377f960206147d93565585d', 'text': 'Chapter 9. Securing 5G Use Cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0ff053d0b7a96d92d1069eef8945a6fc', 'text': 'Secure 5G Smart Factory and Manufacturing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': '693b38087377f960206147d93565585d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fb54abcd768c0c2a68bd1f9cb9cab36f', 'text': 'Critical Infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': '693b38087377f960206147d93565585d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4fac09fb97bb4f4c4bce59daafb5301e', 'text': '5G Vehicle-to-Everything (5G-V2X)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': '693b38087377f960206147d93565585d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '051ac7b436133a8e3b96a940ac985d7c', 'text': 'Standards and Associations', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': '693b38087377f960206147d93565585d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e39137a39f717d93259b0934f7aabeb', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': '693b38087377f960206147d93565585d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '177dc9dbc9e1743e6cf14c0e2c60b899', 'text': 'Key Acronyms', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 10, 'parent\_id': '693b38087377f960206147d93565585d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4e31183850b30ce3e2196e618e11419f', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f820e85b04561f47bfd97ca7cbceaccb', 'text': 'Part III: End to End 5G Security Architecture and Prioritizing Security Investments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '674915b31a28b1f850d05b237d0d8173', 'text': 'Chapter 10. Building Pragmatic End-to-End 5G Security Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': 'f820e85b04561f47bfd97ca7cbceaccb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f55fc1a63f5ece2d71474c42b823b0de', 'text': 'Foundations of 5G Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': 'f820e85b04561f47bfd97ca7cbceaccb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0e2da5d0df83a81f8677065876861594', 'text': 'Key Tenets of 5G Security Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': 'f820e85b04561f47bfd97ca7cbceaccb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6df18b85053dfda15a0153096df3b9f1', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': 'f820e85b04561f47bfd97ca7cbceaccb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '57ecbde77edde51fdfbc4c674fed4f1c', 'text': 'Acronyms Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': 'f820e85b04561f47bfd97ca7cbceaccb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5acf1c2485e5c3565c56515e4f12157b', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': 'f820e85b04561f47bfd97ca7cbceaccb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e5723f2a28380e1ee397a7aac95433b3', 'text': 'Chapter 11. Prioritizing 5G Security Investments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': 'f820e85b04561f47bfd97ca7cbceaccb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3edf0cffa99997c25489d839c9eda416', 'text': 'Method of Prioritizing Security Controls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': 'f820e85b04561f47bfd97ca7cbceaccb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9cae246c1efb89ed256cadf3d58ea577', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': 'f820e85b04561f47bfd97ca7cbceaccb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a8e66b595f82e8b453238a6e2112cd7c', 'text': 'Acronyms Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': 'f820e85b04561f47bfd97ca7cbceaccb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9b9c642c640dff60d8567475a3639e7e', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': 'f820e85b04561f47bfd97ca7cbceaccb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ede1f1c2d57c19d727f842e6251d78ec', 'text': 'Part IV: Emerging Discussions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '47a6748ef4fecc27ff4af4bb767d4f35', 'text': 'Chapter 12. 5G and Beyond', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f9db92885a84661d676b5562fb5c6305', 'text': 'Adoption and Adaptability of 5G and Evolving Technologies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': '47a6748ef4fecc27ff4af4bb767d4f35', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b98c51a1bd29cfd58b4d008ae164972e', 'text': 'Convergence of Wi-Fi and Evolving Cellular Technologies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': '47a6748ef4fecc27ff4af4bb767d4f35', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '84034579c5ad11e9bcfd2c12b7fa3653', 'text': 'Use of AI and ML in Securing 5G and Evolving Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': '47a6748ef4fecc27ff4af4bb767d4f35', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ad680255fb5abfae353241e08a1c8216', 'text': 'Crypto Agility in 5G and Evolving Technologies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': '47a6748ef4fecc27ff4af4bb767d4f35', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd0d72f904554c640de57948e69a60e3e', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': '47a6748ef4fecc27ff4af4bb767d4f35', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '31363999ff78a7c1b082710c1d2edbf3', 'text': 'Acronym Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': '47a6748ef4fecc27ff4af4bb767d4f35', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2bd627c301558e5ac6063999b62c9155', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 11, 'parent\_id': '47a6748ef4fecc27ff4af4bb767d4f35', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7ef6f9c7e9e0f0e8e10ea000dfcab68d', 'text': 'Foreword', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 12, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'acb10f07c24666e2e410dcc472bb790c', 'text': 'Society is about to embark on a digital upgrade—the next generation of the world’s mobile communication infrastructure—5G. Along with new and innovative capabilities, 5G also introduces new security features, vulnerabilities, and risks. 5G does not just represent significantly increased bandwidth and lower latency, but it is expected to fundamentally change the mobile ecosystem with new partnership models, network slicing, massive deployment of Internet of Things (IoT) devices, and ultimately, an increasingly critical dependency on the technology for society to function. Due to this, our ability to secure 5G will directly affect the resilience of critical infrastructure and national security.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 12, 'parent\_id': '7ef6f9c7e9e0f0e8e10ea000dfcab68d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dfc2605bbc2fc78379fede11c23729f3', 'text': 'Some of the security key risks affecting 5G confidentiality, integrity, and availability are supply chain risks, increasing complexity leading to new vulnerabilities, and inherent weaknesses in the standards. The supply chain risks have reached the geopolitical center stage due to the high societal impact of 5G, and this has led to national and EU-level regulations, risks assessments, and GSMA’s accreditation scheme Network Equipment Security Assurance Scheme (NESAS). The inherent increased complexity of 5G leads to a wide range of new potential vulnerabilities that will require increased vigilance from product vendors, service providers, and users alike.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 12, 'parent\_id': '7ef6f9c7e9e0f0e8e10ea000dfcab68d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0573ef9b9b218a39171c45d86cf258ac', 'text': 'In order to manage these risks, 5G is equipped with a broad range of security features and capabilities, and GSMA has outlined a list of critically sensitive functions—virtualization infrastructure, controller, orchestrators, Internet gateways, network slicing, mobile edge computing, routing and switching of IP traffic at the core, database functions, authentication, and access control. As always, a security by design approach following a zero- trust approach, with secure deployments and good operational hygiene, is key to securing the world’s 5G deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 12, 'parent\_id': '7ef6f9c7e9e0f0e8e10ea000dfcab68d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '84971ae980284bc26f754379c636214a', 'text': 'In this book, Pramod Nair guides us through the evolution of cellular technologies from a security perspective, the security architecture, deployment modes and use cases of 5G, as well as discusses end-to-end', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 12, 'parent\_id': '7ef6f9c7e9e0f0e8e10ea000dfcab68d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9d7ef57a93e367fccf3fac2e283175fa', 'text': 'security architecture and prioritizing security investments. His unique outlook as the Lead Security Architect, head of 5G security architecture in Cisco Systems, and from more than 20 years in security allow him to combine a theoretical and applied perspective for the benefit of both business and technical readers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 13, 'parent\_id': '7ef6f9c7e9e0f0e8e10ea000dfcab68d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8a9772192ea53490044fd5ced623aa85', 'text': 'André Årnes, PhD', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 13, 'parent\_id': '7ef6f9c7e9e0f0e8e10ea000dfcab68d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'be36730c195c4035e7cff1f9581ca7ed', 'text': 'Senior Vice President and Chief Security Officer at Telenor Group', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 13, 'parent\_id': '7ef6f9c7e9e0f0e8e10ea000dfcab68d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b080266d4e96ebb4b4f56ab7e7614926', 'text': 'Professor II at the Norwegian University of Science and Technology', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 13, 'parent\_id': '7ef6f9c7e9e0f0e8e10ea000dfcab68d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e0e5447d1a37fd9e545b3e9947a6ad10', 'text': 'Preface', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 14, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '328458b3338ba2dbe78b02b94ad6a6ee', 'text': "5G technology will redefine the way we perceive cellular networks and will touch almost every aspect of our lives. 5G is not about just being faster, bigger, or better; it’s about enabling multiple services that we'll all consume on an everyday basis. It will give rise to a new ecosystem of developers building applications that exploit the openness of 5G to help you develop new use cases for consumption by enterprises and subscribers alike. New features in 3GPP Releases 16 and 17 help further enable new use cases for non-public deployment of 5G by industry verticals and tighter convergence of 3GPP and non-3GPP technologies, bringing in multiple deployment methods—including on-premises, hybrid, and fully public cloud-based deployments. The 5G ecosystem will see a breakout from 3GPP-only based architecture to an open, multi-technology, multi-standard, polyglot ecosystem.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 14, 'parent\_id': 'e0e5447d1a37fd9e545b3e9947a6ad10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d91c4013eb70e47bca27aca60abe2d1', 'text': 'This evolution of the technology landscape also requires an evolution of the security mindset. We should start thinking of security as a foundational layer. It should be one of the primary foundations for any planned 5G use case implementation. This requires embracing multilayered security beyond the requirements in 3GPP specifications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 14, 'parent\_id': 'e0e5447d1a37fd9e545b3e9947a6ad10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '528d5bf85c7c368675b6efc40fafa046', 'text': 'The business operational risk, legal risk, and reputational risk exist not only for the companies providing 5G software and hardware infrastructure, but for all companies, nation-states, and individuals who provide and consume 5G technology.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 14, 'parent\_id': 'e0e5447d1a37fd9e545b3e9947a6ad10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '66d815853a370fd1264e19a123871a73', 'text': 'The time is now to evaluate the cyber risk posture and apply innovative thoughts to how we can approach these challenges today and build for what’s to come tomorrow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 14, 'parent\_id': 'e0e5447d1a37fd9e545b3e9947a6ad10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7114a9d0fefd00427b41babcbfb3080a', 'text': 'Motivation for Writing This Book', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 14, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '417e72265a889adf1a676d27dadae862', 'text': 'Security in evolving cellular technologies is not an easy concept to grasp, as the technologies have evolved rapidly and are becoming increasingly', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 14, 'parent\_id': '7114a9d0fefd00427b41babcbfb3080a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '75133c02a890a5f79ce7a7f70342b3bf', 'text': 'complex and nuanced as they become more open, especially when you add 5G to the mix.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 15, 'parent\_id': '7114a9d0fefd00427b41babcbfb3080a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '905d1b9f05f67060bb36b924f34f18bf', 'text': '5G will also enable enterprises and industry verticals to deploy private 5G/non-public 5G networks (5G NPN networks) on their own, without any integration with service providers. This necessitates private and government sectors to fully understand the 5G threat surfaces, develop methods to mitigate the threats, and prioritize the investments in security.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 15, 'parent\_id': '7114a9d0fefd00427b41babcbfb3080a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e877f2f7ccc679f6ab4427971ddcae06', 'text': 'The existing material on security and cellular technologies is dispersed across many resources and does not cover the end-to-end 5G threat surfaces, threat mitigation, examples of real-life deployment scenarios, and prioritization of security controls based on use cases and deployment scenarios. The learning curve for a person trying to understand the evolution in cellular technologies, new architectures, multiple deployment methods, threat surfaces, and mitigation techniques is extremely steep and sometimes unnerving.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 15, 'parent\_id': '7114a9d0fefd00427b41babcbfb3080a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e0f9daa759e603b094db28b98af7092', 'text': 'It is not surprising that the topic of securing cellular technologies tends to flummox newcomers and even seasoned network security engineers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 15, 'parent\_id': '7114a9d0fefd00427b41babcbfb3080a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '95b0377e9a2d9b8406bb1526ec2fbf3a', 'text': 'This book brings all the information together and arranges the key topics in such a way that they can be easily consumed and understood. The main purpose of this book is to enable any person to understand the key aspects of securing 5G and evolving technologies. This book covers a range of topics; it will take you through the evolution of technologies from 2G to 5G, with deep dives into specific topics, such as securing non-public 5G networks/private 5G deployments and prioritizing security investments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 15, 'parent\_id': '7114a9d0fefd00427b41babcbfb3080a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c433457625fe0f0534ae21e65c8bffec', 'text': 'The goal of this book is to provide pragmatic views on securing 5G and evolving networks. The knowledge and information gathered through numerous customer workshops, brainstorming sessions with service providers, industry verticals, industry experts from multiple vendors, proof of concepts, and lessons learned from actual security deployments for 5G networks are detailed in this book. Discussions with multiple CSOs and CTOs have enlightened me on the key data points required for prioritizing security, which you will see highlighted in this book. Apart from service providers, industry verticals are expected to adopt 5G technology, and this area has been expanded into specific use cases, threats, and mitigation techniques. This book closes with a chapter discussing the key areas of', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 15, 'parent\_id': '7114a9d0fefd00427b41babcbfb3080a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ae8ea87e12f90775e79c22ebe2882a9', 'text': 'security evolution that will motivate you to investigate different aspects of security as the network evolves. It is aimed at helping you create a new mindset while securing your networks of the future.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'parent\_id': '7114a9d0fefd00427b41babcbfb3080a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '222956a718d4d724ce1eefd75725b661', 'text': 'Who Should Read This Book', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9e5881f3bbcbedb9d3777ee061d729c2', 'text': 'I have designed this book so that you can begin without any prior knowledge about 5G or any preceding cellular technologies. This book is written to be suitable for multiple levels of technical expertise, including the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aa241734617eedf1f3881231b57015dc', 'text': '• Security experts looking to understand the history of cellular technology evolution to 5G, key 5G security enhancements, and security challenges', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '544e875d1b9a4874854daec3c04ed8b1', 'text': '• Early-in-career telecom engineers, transport design engineers, and radio engineers looking to design and implement mobile networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3a18ee4c5d2000ae99376e63850b8436', 'text': '• Government departments looking at security impacts of 5G deployment for use cases such as smart city and looking at implementing security measures', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3710521e96a3108da885d1146255a054', 'text': '• Management consultants advising governments and service providers on 5G security strategy', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1c3e827d722d10ff5647188764bcfeed', 'text': '• CSO and CTO teams from service providers looking at securing 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4bc00911cadee1502b4e6c4c0e720eda', 'text': '• CSO and CTO teams from enterprises deploying NPN/private 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c935497942ae3f41e7cad814b26f8948', 'text': '• Enterprise network design and implementation teams deploying NPN/private 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ad1d0b8cd33634bb81156a04b8308c2a', 'text': '• Security architects responsible for securing the mobile infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aec813cedd3cb9465dd4f4c9a0a9e5d1', 'text': '• Enterprise solution architects and enterprise security architects working with enterprises integrated with service provider 5G networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '596681cd3814b55bf6fff5ff4832cd34', 'text': '• Security strategy teams within service providers, enterprise and industry verticals deploying 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8952782eff4a9e75b5815c355646f322', 'text': '• Cloud computing and data center teams involved with 5G strategy and deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 16, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '62e9dd85ff70c37c8f154e06b1985c9c', 'text': "• Enterprise solution and security architects deploying standalone private/NPN 5G or utilizing service providers' 5G slice network", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 17, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '845afbbe889cac3b5936496f2477fe72', 'text': '• Audiences of varying levels of expertise from the military and defense community', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 17, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cb80c8f6751ab437eabdbf0b92147df8', 'text': '• Audiences from industry verticals such as smart manufacturing, critical infrastructure entities and vendors, and autonomous vehicle manufacturers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 17, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d911861c0258c1a1c388b238316b1d8', 'text': '• Cybersecurity vendor product managers looking for use cases or features to enhance security products to cater for secure 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 17, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8845e0a0f58360000095fb46fdd80057', 'text': '• Students who would like to get a quick understanding of cellular technologies and a look at the new features in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 17, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a489ed278df0a9a172338d192717bf95', 'text': 'Throughout the book, you will see practical examples and real-life scenarios of how you might architect a solution to mitigate threats and improve the security posture of your network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 17, 'parent\_id': '222956a718d4d724ce1eefd75725b661', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'text': 'How This Book Is Organized', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 17, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '63ec78cc94ab7d69bd3fe431a946f71b', 'text': 'To allow technical and nontechnical audiences to consume the book in an effective and organized way, it is split into four parts. The parts and chapters cover specific topics.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 17, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '504dd5317919c449b326b9b214544fc9', 'text': 'Part I, “Evolution of Cellular Technologies to 5G, Security Enhancements, and Challenges,” explains the evolution of cellular technologies toward 5G as well as new security enhancements and new security challenges brought in by 5G. It will also take the reader through different deployment modes, including private 5G / non-public networks (NPN). This part will mostly cater to the audience who wants a high-level view of 5G technology and its security aspects. It includes the following chapters:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 17, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '93529fba44508bdcf0438b046cf998c0', 'text': '• Chapter 1, “Evolution from 4G to 5G,” covers the evolution of cellular technologies and will provide you with a basic understanding of the 5G technology features. It will also take you through some of the key enhancements in 3GPP Rel-16 and Rel-17.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 17, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '34d42dfa61dc20e53058537ebfa35ce3', 'text': '• Chapter 2, “Deployment Modes in 5G,” covers the different non- standalone and standalone deployment modes and use cases, which can be mapped to specific deployment modes.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 18, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4f6aea85943b18a65d1eee7b2fae685e', 'text': '• Chapter 3, “Securing 5G Infrastructure,” covers new security enhancements and new security challenges brought in by 5G. It also discusses the reasons why you should have an external layer of security controls, even though 3GPP provides some enhancements in security.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 18, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '436c0b3d3afa0b3d74fd21058292e9e2', 'text': 'Part II, “Securing 5G Architectures, Deployment Modes, and Use Cases,” covers the security controls for 5G network components such as RAN, transport, 5GC, and devices. It then takes you through securing 5G enablers —such as multi-access edge compute (MEC), software-defined networks (SDNs), network slicing, orchestration, automation—and protecting different deployment methods such as on-premises, public cloud, hybrid cloud, including open RAN deployments. It finally covers securing key 5G use cases such as critical infrastructure, vehicle-to-everything (V2X), and smart factory. This part of the book will be of keen interest to readers who would like to deep-dive into the security aspects of 5G and its key use cases. It includes following chapters:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 18, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b1a43e931cff60bb1ee1cb1e43413035', 'text': '• Chapter 4, “Securing RAN and Transport Deployments in 5G,” covers the 5G RAN and transport threat surfaces and threat mitigation for the 5G public and non-public deployments, including open RAN. This chapter also takes you through some real-world attacks and mechanisms to mitigate them.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 18, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '90bdd251f67f1820b2c2c03403855fce', 'text': '• Chapter 5, “Securing MEC Deployments in 5G,” covers various MEC deployment models, network functions deployed in the private and public cloud based MEC, it’s threat surfaces, and methods to mitigate the threats. The chapter also provides some real-world risk and risk mitigation scenarios.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 18, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '669ed7c72933d59286ec7f4af7e5afd2', 'text': '• Chapter 6, “Securing Virtualized 5G Core Deployments,” covers the threats due to virtualized 5G Core deployments and new methods of software development and deployment. This chapter also provides some key recommendations to secure your virtualized 5GC deployments with vendor-agnostic approaches and includes some real- world scenarios.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 18, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '750148553c5c914a67b05c15656c08f7', 'text': '• Chapter 7, “Securing Network Slice, SDN, and Orchestration in 5G,” covers network slicing and enablers of network slicing such as software-defined networks (SDNs), orchestration, and automation. The chapter also explains the threat surfaces and threat mitigations specific to network slicing and its enablers. This chapter also delves into the network slice as a service (NSaaS) offering, its threat surface, and methods to mitigate the threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 19, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e8e6645b7ff89150ee7969cd723558d9', 'text': '• Chapter 8, “Secure Massive IoT Deployments in 5G,” covers the risks related to IoT devices and related connectivity and management. The chapter then goes on to explain different security mechanisms and best practices to secure your network from any IoT device-based attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 19, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ccc28752176c7db679c5d084b663b47e', 'text': '• Chapter 9, “Securing 5G Use Cases,” covers critical infrastructure, V2X, and smart manufacturing use cases, which use different types of IoT devices—some smart, some semi-smart —as well as non-smart devices. The chapter takes you through the risks within these three use cases and methods to mitigate the risks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 19, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9247ab74d4979bff1eb0210d7e215c7f', 'text': 'Part III, “End-to-End 5G Security Architecture and Prioritizing Security Investments,” provides an overview of the various security recommendations for end-to-end 5G security and discusses the factors based on which certain security controls can be prioritized among other security controls for 5G networks. This part will be of keen interest to an audience who would like to have an end-to-end view of security and understand the methods to prioritize investments in security. It includes following chapters:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 19, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7080a598931f27596299bffc61a84bd9', 'text': '• Chapter 10, “Building Pragmatic End-to-End Security Architecture for 5G,” covers the key building blocks for creating an end-to-end security layer for 5G deployments. This chapter also provides you with a checklist for each of the 5G domains and includes zero-trust design principles.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 19, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '722aca4216fdbf93de9cc070be63cf69', 'text': '• Chapter 11, “Prioritizing 5G Security Investments,” covers the considerations and recommendations for prioritizing investments to secure your 5G network. This chapter takes two primary scenarios— one related to a service provider providing mobile service, and the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 19, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd04a52d800cb806a6377bfb0cf8e7b8f', 'text': 'other related to the non-public deployment methods for industry verticals and enterprises.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 20, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '49bbc5131aecb964870f1a7ae3ce6cc7', 'text': 'Part IV, “Emerging Discussions,” takes you through the topics aimed at new features being discussed for 5G and evolving architectures, security enhancements using machine learning (ML) and artificial intelligence (AI), and the method to make your network quantum safe. This part will be of keen interest to readers who would like to understand the key discussions in the security industry around 5G and evolving technologies. It includes following chapter:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 20, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e83541f21522dda6ebd337a692f722f1', 'text': '• Chapter 12, “5G and Beyond,” covers the adoption and adaptation of 5G Standalone technology with new use cases, convergence of non- 3GPP and 3GPP technologies, application of AI and ML in securing 5G and evolving technologies, and the importance of deploying crypto-agile mobile networks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 20, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '90f38fd17d2e0e510876226a27badbdc', 'text': 'Due to ongoing developments, Chapter 12 will occasionally be updated with relevant new content and insights on the book’s website at www.informit.com. To access the chapter, start by establishing a login at www.informit.com and then register your book. To do so, simply go to www.informit.com/register and enter the ISBN of the print book (9780137457939). Answer the challenge question as proof of purchase. Click the “Access Bonus Content” link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 20, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c09e9a372cf3af044ac9e5dd0ff36ea6', 'text': 'Please note that this book is written with a vendor-neutral approach, and it does not give recommendations on what vendor should be deployed. Each service provider or industry vertical planning to deploy 5G can evaluate the security controls required and make decisions based on their own criteria, circumstances, and targeted use cases. This book covers the details of the security controls, required features, and functions required for securing 5G and evolving networks, allowing you to make better informed decisions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 20, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '02aff8bdd4665bc47e67fbf70204f847', 'text': 'Happy reading, and I hope you enjoy this book as much as I enjoyed writing it!', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 20, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bab60867a29f2ec6756ada2d1c2ed883', 'text': 'Register your copy of Securing 5G and Evolving Architectures on the InformIT site for convenient access to updates and/or corrections as they', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 20, 'parent\_id': 'a94af9b347f4739cacc0c658ce2855b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d67cab0e5376bfbc558b2a7b50bead3', 'text': 'become available. To start the registration process, go to informit.com/register and log in or create an account. Enter the product ISBN (9780137457939) and click Submit. Look on the Registered Products tab for an Access Bonus Content link next to this product, and follow that link to access any available bonus materials. If you would like to be notified of exclusive offers on new editions and updates, please check the box to receive email from us.', 'metadata': {'links': [{'text': 'informit . com / register', 'url': 'http://informit.com/register', 'start\_index': 59}], 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 21, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1071a59d2fc03cc79ae6509666eddff9', 'text': 'Acknowledgments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 22, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'effd4d126e6597eff7b2b75bdf98c6dc', 'text': 'I would like to acknowledge the tremendous support I received from the Cisco staff, especially my management team and colleagues.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 22, 'parent\_id': '1071a59d2fc03cc79ae6509666eddff9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4f856723ae07ca83d1383be6ee8064d4', 'text': 'Similarly, I would like to thank the reviewers, Keith O’Brien and David Hucaby, for their comments, feedback, and insights that enriched the content of this book.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 22, 'parent\_id': '1071a59d2fc03cc79ae6509666eddff9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cd3861d298495c7c0c1b8959a5683581', 'text': 'I would like to thank Dr André Årnes, PhD, Senior Vice President and Chief Security Officer at Telenor Group and Professor at the Norwegian University of Science and Technology, for writing the foreword.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 22, 'parent\_id': '1071a59d2fc03cc79ae6509666eddff9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2b52fec0c1c54a19423b6f6338848b12', 'text': 'I would like to extend my appreciation to the people from multiple companies who provided constructive comments during those numerous 5G security customer workshops and brainstorming calls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 22, 'parent\_id': '1071a59d2fc03cc79ae6509666eddff9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a588222e0575edd0cd9f1199ae7385d6', 'text': 'I would like to thank the executive technical editor, Davis Nancy, for her guidance, feedback, and massive support. I would also like to extend my thanks to the Cisco Press team, especially to Chris Cleveland, the development editor, for his robust guidance throughout the editing process.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 22, 'parent\_id': '1071a59d2fc03cc79ae6509666eddff9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '817c00b257dbf26c7de7f769c76751a4', 'text': 'Finally, I would like to thank the many standards organizations, technologists, security experts, and industry peers who continue to contribute to the fields of both mobile communications and security.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 22, 'parent\_id': '1071a59d2fc03cc79ae6509666eddff9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e6c9cf9e53ddee062827b071bc28ec21', 'text': 'About the Author', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 23, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e4be3d775c2e3c85c98ccda0c0b2c0ae', 'text': 'Pramod Nair is a Lead Security Architect at Cisco Systems focusing on service providers. During his 20 years of experience in the industry, Pramod has worked in multiple areas, including research and development, designing end-to-end mobile networks, and technical consulting on military and defense projects.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 23, 'parent\_id': 'e6c9cf9e53ddee062827b071bc28ec21', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ddf31853be2406845051e7bfc7768cb9', 'text': 'Among other responsibilities in his current role within Cisco, Pramod leads 5G Security Architecture, driving its adoption globally, and has been instrumental in architecting secure next-generation networks for customers across the globe. He is a regular speaker on the subject at large conferences and industry events.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 23, 'parent\_id': 'e6c9cf9e53ddee062827b071bc28ec21', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0b1c47200824570249a2ee790cc86338', 'text': 'Pramod is an active member of the security community. His role is to help mobile network providers, service providers, industry verticals, the national security and defense sectors, and other agencies dedicated to securing critical infrastructures. He is also deeply involved with industry trade organizations, has co-chaired the 5G security white paper within the 5GAmericas work group, and works with the National Institute of Standards and Technology (NIST) on 5G security.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 23, 'parent\_id': 'e6c9cf9e53ddee062827b071bc28ec21', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '02570b90b8fcb4a8c74877498a0bfc21', 'text': 'Pramod holds a patent in fraud detection and has published various white papers and articles covering security-related topics.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 23, 'parent\_id': 'e6c9cf9e53ddee062827b071bc28ec21', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6744764d71acda0e40b3335e3f69cdb6', 'text': 'Part I: Evolution of Cellular Technologies to 5G: Security Enhancements and Challenges', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 24, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '98907bc956fc64f40ea5b0321106e417', 'text': 'Chapter 1. Evolution from 4G to 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2877e19518cd8b258ac3f93339b2599', 'text': 'After reading this chapter, you should have a better understanding of the following topics:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2c91c2b0e0d122c6c635aa4081332a04', 'text': '• Evolution of cellular technologies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '03271992a547814a91ccacc3ac32e921', 'text': '• Enhancements in 5G as compared to 4G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b052551ae4d4dd8433b1a42f00559e81', 'text': '• Key 5G features and enhancements in 3GPP Releases 15, 16, and 17', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0d1463b3badbfa39da7cedcf4bd352d9', 'text': '• Key 5G Advanced features and enhancements under study in in 3GPP Releases 18', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a58e558e83e5fc886fd7304afa863979', 'text': 'This chapter takes you through the evolution of cellular technologies and provides you with a basic understanding of 5G technology features.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0b2229f9cad0e917e7c0d57d1ea383ab', 'text': 'This chapter will be of particular interest to the following individuals and teams from enterprise/5G service providers deploying 5GC and cybersecurity vendors planning product developments for 5G security use cases:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cd3821073b16b542bd6c949a16120ce1', 'text': '• Security leaders within government organizations who would like a quick look into the brief history of cellular communications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '04dc59773352ffe1a181ca935986c436', 'text': '• Teams from enterprise and industry verticals who want an understanding of cellular technologies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '02fad09918f9654dfec85c67e12d6260', 'text': '• Enterprise cybersecurity vendor security architects looking to understand the evolution of cellular technologies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '171c84cd342e00187fa669062e5db483', 'text': "• Cybersecurity vendor security architects and product managers looking to understand what's new in 3GPP Releases 15 and 16 and what's planned in Release 17", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8cd66ed38409137e1f13cc4568f2d6bb', 'text': '• Cybersecurity students who would like to get a brief understanding of cellular technologies and new features in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '09985caf835635619f2f53a3d16ba4b3', 'text': 'In mobile technologies, the “G” in 1G, 2G, 3G, 4G, and 5G refers to “Generation,” where there has been a major shift in the capabilities offered in terms of spectrum efficiency, higher throughput, making the architecture more “flat,” and enhanced algorithms in the air interface for providing better', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 25, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '782fc037254993760a6d960d1ebb8502', 'text': 'security. 1G was based on analog technology, and 2G was the first digital technology to be used in mobile cellular communication.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 26, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8dbc68777abc8dfd3b20bc238a0cae77', 'text': 'The foundation of 4G was set by International Telecommunications Union– Radio communications sector (ITU-R) around 1998. In 2009, 4G was established and called Long Term Evolution before eventually being called 4G (pure marketing), although it did not meet the criteria of 1Gbps for low- mobility use cases (pedestrian users). In 2011, LTE-Advanced (LTE-A) fulfilled the criteria set by ITU-R and specified in Releases 8 and 9 of Third- Generation Partnership Project (3GPP) and was actually “true 4G.” The U.S. Defense Advanced Research Projects Agency (DARPA) had also envisioned 4G by using end-to-end IP networking and distributed architectures.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 26, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2b5101ef39d974198c924dd24be4e36', 'text': 'Figure 1-1 illustrates the evolution of cellular digital networks from 2G to 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 26, 'parent\_id': '98907bc956fc64f40ea5b0321106e417', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'cd2c20660b37147a66da5713f5ffee34', 'text': '[ A 2020 ((A)) L SA 2019 I E-A 2011 [ E 2009 ((A)) (S ((A)) 2001 PS L OP (S ((A)) 1992 PS D AR R (S Circutt Sﬁwilt‘cr)edl IMME:I Mob@ty Mapnalge‘ment Entty', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 27, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '83d65015c040b813d46b7d58828827d3', 'text': '(S Circutt Sﬁwilt‘cr)edl', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 27, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'afa62a0e3cce7e2ab546de776490bce1', 'text': 'IMME:I Mob@ty Mapnalge‘ment Entty', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 27, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4cd5d210a676b5ba330855ec42c9f371', 'text': 'Figure 1-1 Evolution from 2G to 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 27, 'parent\_id': 'afa62a0e3cce7e2ab546de776490bce1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '593711176629f2745d49f63da0b23755', 'text': 'Mobile technologies had come a long way from 1G in 1981, 2G in 1992, 3G in 2001, to 4G in 2009/2011(LTE-A). As shown in Figure 1-1, 4G brought a shift in designing the mobile network, as it was based on all Internet Protocol (IP) deployment, allowing better throughput due to reduced latency in the back haul, better modulation techniques, advanced dynamic channel allocation, and adaptive traffic scheduling. Advanced antenna systems such as Multiple Input Multiple Output (MIMO) with beamforming helped achieve better throughput, but its use was restricted due to cost and was aimed at specific dense clusters that required high throughput. 4G also brought in a major shift in the network design, as it moved away from the requirement of having both circuit-switched and packet-switched networks and enabled the simplification of network architecture to a purely packet switched (PS) all-IP flat network architecture with reduced latency. For example, the following systems used separate circuit- switched networks for voice and packet-switched networks for data:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 28, 'parent\_id': 'afa62a0e3cce7e2ab546de776490bce1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b426b188d498a2ebbf903bb579773909', 'text': '• 2.5G, also called General Packet Radio Service (GPRS)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 28, 'parent\_id': 'afa62a0e3cce7e2ab546de776490bce1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ee9c51aa5f960a2104130c7b324b2f3', 'text': '• 2.75G, also called Enhanced Data Rates for GSM Evolution (EDGE)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 28, 'parent\_id': 'afa62a0e3cce7e2ab546de776490bce1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a217cb039906eedc7604cc063445bd8', 'text': '• 3G systems', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 28, 'parent\_id': 'afa62a0e3cce7e2ab546de776490bce1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7c6ee257120c969da4ae4d39207fa8ac', 'text': 'For a service provider, 2G and 3G systems required two separate sets of equipment in parallel, as they had separate circuit switch (CS) traffic for voice and packet switch (PS) traffic for packet data. The IP-based flat network architecture in LTE helped to reduce costs and complexity by replacing the separate circuit- and packet-switched networks with a single Evolved Packet Core (EPC), which also had the capability to support handovers from legacy 2G and 3G technologies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 28, 'parent\_id': 'afa62a0e3cce7e2ab546de776490bce1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd5dbd8898d651f1cada6ef9e707eac13', 'text': 'Mobile Network Evolution from 4G to 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 28, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cf625429d9dfd6b6c026af3a7cfdca61', 'text': '5G is the successor of 4G technologies, and it defines a system that uses 5G New Radio (NR) software. The standards are set by 3GPP, and the minimum specifications were set by the International Telecommunications Union (ITU) International Mobile Telecommunications–2020 (IMT-2020) standard in 2015. 5G is not just going to be about high-speed data connections for enhanced mobile broadband; it will enable several new capabilities that can cater to several new enterprise use cases. 5G will not just be about serving consumer/enterprise subscribers with high-throughput connectivity. 5G will enable new revenue avenues and opportunities for operators by being able to cater to requirements for several new enterprise use cases. The first NR', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 28, 'parent\_id': 'd5dbd8898d651f1cada6ef9e707eac13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1176e0f47560c4ca30f3c7f71a1682f0', 'text': 'specification was made in 2015, whereas the phase of 3GPP 5G specifications in Release-15 was completed in 2019 (also referred to as “Phase 1” standardization of 5G). The initial Phase 1 deployment of 5G was based on a software upgrade of 4G LTE infrastructure and was called Non-Standalone (NSA) mode, which depended on an existing 4G LTE network for control plane signaling and used 5G NR for the user plane. Phase 2 is based on Standalone (SA) mode with 5G packet core network (5GC) providing the control plane and 5G NR providing the user plane.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 29, 'parent\_id': 'd5dbd8898d651f1cada6ef9e707eac13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '362ec63d4668423e03ae4cd5b57a3133', 'text': 'Figure 1-2 illustrates the high-level 5G architecture with comparisons to 4G architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 29, 'parent\_id': 'd5dbd8898d651f1cada6ef9e707eac13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '71c7114c090c83217789cadf6a01cc27', 'text': 'R 0 46 () Teleo DC 4G Radio Backend Transport o= 46 Mobile Broadband g () & Vioice ode (eNB = Service Provider 4G Teleo DC Applications and Internet', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 29, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c2d01f870f3e5d972a9716048d275e91', 'text': '0 46 () Teleo DC 4G Radio Backend Transport o= g () ode (eNB = Service Provider 4G Teleo DC Applications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 29, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6c5bbf303bacf314ed7656b5b2fdef55', 'text': 'S R R S PR', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 29, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '08abff3eca656e232bd22a086286bec6', 'text': 'Disaggregated RAN Virtualized Cloud Native 5G network functions with APIs 56 Publlc Cloud k N 56 Mobile Broadband / Internet / roaming Transport ﬂ Transpcrt ﬂ panes 5G Radio Node (gNB) \_ ﬂ MEC Centralized 56 Service Provider Applications and Internet Network Functions Ulra Low Latency use cases [y Distributed 5G network JEaoA', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 29, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Header', 'element\_id': 'd287fe50a8e20c412c3d2b534aecfd9e', 'text': 'Figure 1-2 Comparison of 5G and 4G Architectures', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 30, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2038d96cfdfa40279897bd735c6fb999', 'text': 'Apart from higher data rate/throughput and utilizing a new spectrum, the key differentiators and technology evolutions in 5G as compared to 4G are discussed in the sections that follow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 30, 'parent\_id': 'd287fe50a8e20c412c3d2b534aecfd9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e5dfd67d58d7146869fc7c2044c74a13', 'text': '5G New Radio Features', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 30, 'parent\_id': 'd287fe50a8e20c412c3d2b534aecfd9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8c6e77c16de0790acb3269eb18b95900', 'text': 'New Radio (NR) for 5G should support the following key requirements:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 30, 'parent\_id': 'e5dfd67d58d7146869fc7c2044c74a13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8514ade5e4b2ce4f475395f585df31b2', 'text': '• The ability to handle high data rates and a wider bandwidth', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 30, 'parent\_id': 'e5dfd67d58d7146869fc7c2044c74a13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2466190ff5f0f025d19fa3242c63f6f2', 'text': '• Support for ultra-reliable low-latency communications (URLLC) with fast short bursts of data', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 30, 'parent\_id': 'e5dfd67d58d7146869fc7c2044c74a13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '69fa595e3b6407d8bda338653286d6e9', 'text': '• Support for energy efficient communications for low powered devices catering for internet of things (IoT)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 30, 'parent\_id': 'e5dfd67d58d7146869fc7c2044c74a13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0d142d84fc79f3e6272482574a1701e7', 'text': 'The requirements are met by using cyclic prefix-based orthogonal frequency- division multiplexing (OFDM), which is the same waveform LTE uses for downlink. For downlink, only cyclic prefix-based OFDM (CP-OFDM) is used. While for uplink, both CP-OFDM and Discrete Fourier transform spread OFDM (DFT-S-OFDM) can be used. Compared to CP- OFDM, DFT-S-OFDM has the merit of a lower peak-to-average ratio.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 30, 'parent\_id': 'e5dfd67d58d7146869fc7c2044c74a13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8c2b2e6a42da32033be704328c794e24', 'text': 'Dynamic Spectrum Sharing (DSS) and Flexible NR Protocols', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 30, 'parent\_id': 'd287fe50a8e20c412c3d2b534aecfd9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58996780a592d2153070f0b06950f984', 'text': 'During the initial stages of 5G adoption, Non-Standalone (NSA) mode is the preferred mode of deployment for service providers, before transitioning to the full-fledged 5G Standalone mode of deployment. The 5G NR can adapt to existing 4G deployments and share the spectrum used exclusively by 4G today, using a mechanism called Dynamic Spectrum Sharing (DSS). DSS allows the service providers to share the spectrum between 4G and 5G without having to re-farm the 4G spectrum. This method is therefore spectrum efficient and facilitates a smooth transition to 5G SA. In DSS, the 5G NR device, such as user equipment (UE), will have two active radios—one for 4G and the other for 5G NR—that detect the synchronization signal blocks (SSB) to access the network. SSB is sent periodically by the network within the 4G multimedia', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 30, 'parent\_id': '8c2b2e6a42da32033be704328c794e24', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '611479ec4a027ef8af844c99357f57b4', 'text': 'broadcast single-frequency network (MBSFN) subframes to maintain synchronization in time and frequency.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 31, 'parent\_id': '8c2b2e6a42da32033be704328c794e24', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f2b500ffdde0a7c4c2417235b967ebcd', 'text': 'Operating Spectrum and Bandwidth', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 31, 'parent\_id': 'd287fe50a8e20c412c3d2b534aecfd9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '74f216874fde1d1ff03ebeae75db9fe6', 'text': 'The frequency range in which 5G NR can operate is split between FR1 and FR2, as documented in Table 1-1.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 31, 'parent\_id': 'f2b500ffdde0a7c4c2417235b967ebcd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'b76311b9021772fc31f2e333281234cd', 'text': 'Frequency Range Designation Frequency Range FR1 410-7125 MHz FR2', 'metadata': {'text\_as\_html': '<table><thead><tr><th></th><th></th></tr></thead><tbody><tr><td></td><td></td></tr><tr><td></td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 31, 'parent\_id': 'f2b500ffdde0a7c4c2417235b967ebcd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '43674f20fd87910362285f3581845793', 'text': 'Table 1-1 5G Frequency Range', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 31, 'parent\_id': 'f2b500ffdde0a7c4c2417235b967ebcd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ad3e32bf059ba0e4f41b6082b52f355d', 'text': '5G NR also supports hierarchical system bandwidth from 5 MHz to 100 MHz for FR1 and from 50 MHz to 400 MHz for FR2, respectively, as indicated in Table 1-2.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 31, 'parent\_id': 'f2b500ffdde0a7c4c2417235b967ebcd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'ef371b2076786e7c980b7da82a8d30f1', 'text': 'Frequency Range Designation Bandwidth', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Frequency Range Designation</th><th>Bandwidth</th></tr></thead><tbody></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 31, 'parent\_id': 'f2b500ffdde0a7c4c2417235b967ebcd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6ce25756754913b742f428fb09fbf9ff', 'text': 'Table 1-2 5G Bandwidth', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 31, 'parent\_id': 'f2b500ffdde0a7c4c2417235b967ebcd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '678436dde20e67a44bc65232be8f139e', 'text': 'Massive MIMO', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 31, 'parent\_id': 'd287fe50a8e20c412c3d2b534aecfd9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9e2300305ab0c25159867e34d5c8130e', 'text': "One of the key enablers for 5G's higher data rates is Multiple Input Multiple Output (MIMO). MIMO as a technology is not new and has been around for quite some time. The key reason MIMO is important in 5G is due to the use of higher frequencies in 5G, which leads to higher losses and therefore lower coverage. Massive MIMO with its higher number of transceivers will help in improving capacity, coverage, and spectrum efficiency as well as the user experience. Apart from the higher number of transceivers, beamforming will", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 31, 'parent\_id': '678436dde20e67a44bc65232be8f139e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2cf49d709f0bc4d017b34c89645c65b3', 'text': 'also help in identifying coverage requirements for moving users and optimizing the offered coverage and capacity.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 32, 'parent\_id': '678436dde20e67a44bc65232be8f139e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1f579e3d5f9ef384e54d9582dd691cd0', 'text': 'Disaggregated Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 32, 'parent\_id': 'd287fe50a8e20c412c3d2b534aecfd9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '285b63e500c57c94fc8851d705ccc790', 'text': '5G introduces disaggregation of network functions in the Radio and Packet Core domains, which is a dramatic departure from proprietary closed hardware and software sourced from a single vendor toward completely decoupled, open source network functions that are then combined to provide the 5G-specified services.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 32, 'parent\_id': '1f579e3d5f9ef384e54d9582dd691cd0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '84f8fbd174f66b392510a206dce56101', 'text': 'Figure 1-3 illustrates the functional split of Next-Generation RAN (NG-RAN) and 5G Core, along with their main tasks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 32, 'parent\_id': '1f579e3d5f9ef384e54d9582dd691cd0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'bc1d2d97c757a135eea91787ba6b13f6', 'text': 'AVF =13 NB UE IP address allocation : d i il PDU Session Control | UPF i i Dynamic Resource Allocation i POU Handling NG-RAN 5GC Source: 3GPP TR 21.915 UPF: User Plane Function NAS: Non-Access Stratum RRM: Radio Resource Management AMF: Access and Mobilty Function PDU: Protocol Data Unit SMF: Session Management Function 5GC : 5G Packet Core UE : User Equipment aNB: Next Generation NodeB NG-RAN: Next Generation Radio Access Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 33, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '7848e1a2e494411d2a54ff8720f56f17', 'text': 'Source: 3GPP TR 21.915 UPF: User Plane Function NAS: Non-Access Stratum RRM: Radio Resource Management AMF: Access and Mobilty Function PDU: Protocol Data Unit SMF: Session Management Function 5GC : 5G Packet Core UE : User Equipment aNB: Next Generation NodeB NG-RAN: Next Generation Radio Access Network', 'metadata': {'text\_as\_html': '<table><tbody><tr><td>Source; 3GPP TR 21.915</td><td>UPF: User Plane Function</td><td>NAS: Non-Access Stratum</td></tr><tr><td></td><td>AMF: Access and Mobilty Function SMF: Session Management Function</td><td>Management PDU: Protocol Data Unit</td></tr><tr><td></td><td>5GC : 5G Packet Core</td><td>UE : User Equipment</td></tr><tr><td></td><td>aNB: Next Generation NodeB</td><td>NG-RAN: Next Generation Radio Access Network</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 33, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '950374f6da54812e9ed03552a5b07e7c', 'text': 'Figure 1-3 Functional Split of NG-RAN and 5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 33, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1fcc5c111831519015b83d319dc1bdfe', 'text': 'As shown in Figure 1-3, the next-generation NodeB (gNB), which is the next generation base station supporting the new 5G New Radio (NR), performs the access node–related tasks, including radio resource management, radio bearer, connection, scheduling, and admission control for the UE. In the 5GC, Access and Mobility Function (AMF) caters for control plane, Session Management Function (SMF) caters for session establishment, and User Plane Function (UPF) handles the user plane.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 34, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '46cfc9bb1488ba946fb612a93b3ca207', 'text': 'Apart from the functional split between NG-RAN and 5GC, as illustrated in Figure 1-3, the gNB can be deployed as virtual centralized unit (VCU) and virtual distributed unit (VDU) instances on commercial off-the-shelf (COTS) hardware, due to the disaggregation and decomposition introduced by 5G, as shown in Figure 1-4, thus enabling flexible 5G deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 34, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd47187859a5f9d4cdccbe4ec467d11f3', 'text': '—\_—— e —— (« A)) - ——— e —— gNB NS ————— - - Disaggregation N =3 Hardware Software Decomposition of RAN Functions vCU vDU', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 35, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0b1381786fb48f74657f0b8655936b5f', 'text': 'Figure 1-4 Disaggregation and Decomposition of gNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 35, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '279043c4f0f2e3d2f5ed70a6f1372ca8', 'text': 'The CU processes non-real-time protocols and services, and the DU processes PHY-level protocol and real-time services. This allows you to build an end-to- end public or non-public 5G network by employing virtualized network functions from multiple vendors and deploying it on COTS servers using merchant silicon.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 35, 'parent\_id': '0b1381786fb48f74657f0b8655936b5f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0e0ed35f24544a6b8581d11f2defbee6', 'text': 'Network disaggregation eliminates vendor lock-in and enables you to select the best combination of hardware and software vendors based on the offered strengths and features of their respective solutions. The decomposition and disaggregation of 5G enables a major architectural shift to an edge infrastructure that combines decomposed subscriber management with access functionality. This shift will also apply to wireline networks with increasing adoption of the 5G Fixed Access Networks. Figure 1-4 illustrates the disaggregation and decomposition of Radio Access Network (RAN) functions. Disaggregation in 5G brings you lots of flexibility because it fundamentally changes the way networks are procured, built, and operated. Here are some of the benefits:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 36, 'parent\_id': '0b1381786fb48f74657f0b8655936b5f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ce74629e3e12edb29c1baf6128fd0a7a', 'text': '• Efficient partitioning of network functions and resources to support the 5G use cases such as enhanced mobile broadband (eMBB), ultra-reliable low- latency communication (URLLC), and Internet of Things (IoT) by using technologies such as software-defined networking, edge computing, service function chaining, and service orchestration.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 36, 'parent\_id': '0b1381786fb48f74657f0b8655936b5f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dabe2c1dda537771a12fee2757b87820', 'text': "• In 5G deployment models such as Cloud RAN (C-RAN), pre-provisioning of baseband resources network isn't required for the maximum capacity of the site. You can use baseband resource pooling provisioned for the traffic profile of the entire network. These traffic profiles can be scaled up or down during peak-hour usage or in the case of high-traffic events.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 36, 'parent\_id': '0b1381786fb48f74657f0b8655936b5f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8e291227a8dfc42e33fc52022fb73746', 'text': '• Scalability to quickly and cost effectively adapt to various network topologies and use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 36, 'parent\_id': '0b1381786fb48f74657f0b8655936b5f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '162ac21dc0cd6419415254c998149a9e', 'text': '• Enhanced network availability and reliability already built into NFV technologies such as OpenStack, the virtual infrastructure manager, and service orchestrator.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 36, 'parent\_id': '0b1381786fb48f74657f0b8655936b5f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a90922098b32e2dfe62da2bd4e91217d', 'text': '• Disaggregation of the hardware from the software using commercial off- the-shelf, high-processing density hardware and open interfaces.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 36, 'parent\_id': '0b1381786fb48f74657f0b8655936b5f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b718af8e354b1a165a893ec2875e1f77', 'text': '• Enablement of advanced algorithms such as cooperative multipoint and inter-site carrier aggregation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 36, 'parent\_id': '0b1381786fb48f74657f0b8655936b5f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '53849a37b8a17d3635b4346405b48a22', 'text': 'As mobile technologies evolved from one generation to the next, the functions performed by base stations and other devices have been distributed using cloud technologies. Cloud-RAN decouples the baseband processing from the radio units, allowing the processing power to be pooled at a central location, thus reducing the required redundancy. One of the most important aspects of C- RAN architecture is the splitting of base station functions at distributed', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 36, 'parent\_id': '0b1381786fb48f74657f0b8655936b5f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5a08be42448fdebcf1cd4ee89c31e989', 'text': 'locations and centralized C-RAN servers. There are eight standardized options for this split, with two (options 2 and 7) being seen most frequently. Figure 1-5 illustrates the functional split consideration in the 5G RAN.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 37, 'parent\_id': '0b1381786fb48f74657f0b8655936b5f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e92e8a92b99cec80fa318f6c817eeb5a', 'text': 'Functions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 37, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '601754e496c03dfa3e931ec77295b02f', 'text': 'Functions e — — - | Split Option Option 1 Py T Option 2 e e — — — Option 3 L e [ Option 4 - e == Option 5 gNB - N = — — = Option 6 Option 7a VN Option 7b A TR, O 0 o NP L Tl L Option 7c | Option 8 ‘ A - -', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 37, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '806c34341f08e65e775e2f21f032c08b', 'text': 'Figure 1-5 Functional Split Options in 5G RAN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 37, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '69076377c334bde8b97dd6699dc2fca9', 'text': 'The chosen radio split option will have a direct impact on your transport (xHaul) design and deployment because the transport requirements vary dramatically with radio split options; therefore, you should consider your existing transport design, its capabilities, and future enhancements in your transport layers before you decide on the radio split options. The 3GPP specifications 38.801 and 38.816 provide additional details about the radio split options.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 37, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '589e9fbeeaa1f42688fdf29c729444eb', 'text': 'Flexible Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 38, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '038dff49fbbe2cdaca2584d04e6569ae', 'text': 'Traditional mobile networks are based on defined perimeters, where most of the mobile packet core functions are centralized. 4G did bring in Control Plane and User Plane Separation (CUPS), but it was not used much due to limited use cases and advantages. 5G SA Packet Core is inherently equipped with several new built-in capabilities so that you have flexibility and capability to face new challenges thrown open by the new set of requirements for varying new use cases in 5G. The network functions in the new 5G Core are broken down into smaller entities, such as the Session Management Function (SMF) and User Plane Function (UPF), which can be used on a per-service basis. Gone are the days of huge network boxes—welcome to services that can be deployed on private cloud and public cloud and automatically register and configure themselves over the service-based architecture (SBA), which is built with new functions like the Network Resource Function (NRF) that borrow their capabilities from cloud-native technologies. This flexible architecture will equip you with more capabilities to cater to enterprise customer needs to support their current use cases as well as new use cases. Enterprise and industry verticals can also deploy their own standalone non-public network (NPN) or public network integrated non-public network (PNI-NPN) to fulfill the use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 38, 'parent\_id': '589e9fbeeaa1f42688fdf29c729444eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a97947e89e5ef2fd5c0faf1179c36d52', 'text': '5G Non-Standalone (NSA) Solution', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 38, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '16a0c2ead79ab56b062717911f4d52a2', 'text': 'In Non-Standalone (NSA) architecture, the 5G RAN and its NR interface are used in conjunction with the existing LTE and Evolved Packet Core (EPC) infrastructure core network (respectively 4G Radio and 4G Core), as shown in Figure 1-6, thus making the NR technology available without network replacement.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 38, 'parent\_id': 'a97947e89e5ef2fd5c0faf1179c36d52', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a54581e655ef47304c97e5d1185b55b9', 'text': "e ——————————————— EPC € (4G LTE Evolved Packet Core) MME / SGW E [ S P —— | ——— [T / ~ S1-U v ~ | ‘\\// EUTRA - NR 5G Base Station §1-C o] SN 7 S;;CIIX 2‘ :-.:U:B ‘-Sj.f 'X @ \\\\ / 4G Base Station N \\ eNB - X2 eNB MN NN", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 39, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '33ebc530aca9124962f3da1c550cc8f5', 'text': 'MME - Mobility Management Entity', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 39, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9a930fc1f119332639011be5f9fedbff', 'text': 'SGW - Serving Gateway', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 39, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e62eec8d26bf81d81f517dc06fbe8b37', 'text': 'eNB - 4G base station', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 39, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '48bea5de2f1841c24a994a26f2e1a16b', 'text': 'en-gNB - EUTRA-NR Dual Connectivity 5G NR base station', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 39, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9ff47cd921870844b82d6c29a268f88a', 'text': 'MN - Master Node', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 39, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e76cbe90f2d3e0c1e9c4cd3b7e91a9f5', 'text': 'SN - Secondary Node', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 39, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e8fc4656cc5607388f799c3b397f2bdf', 'text': 'Figure 1-6 Non-Standalone (NSA) 5G Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 39, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ff4d2edc13d88ec3c766c8776df5e018', 'text': 'In this configuration, only the 4G services are supported but enjoy the capacities offered by the 5G New Radio (lower latency and so on). The NSA is also known as E-UTRA-NR Dual Connectivity (EN-DC). This is where you will leverage your existing EPC (4G) Packet Core to anchor the 5G NR using the 3GPP Release 12 dual connectivity feature. This will help you with aggressive 5G launch needs to launch 5G in a shorter time and with less cost. The 5G NSA solution will suffice for some initial use cases. However, 5G NSA has limitations with regard to getting a much cleaner, truly 5G-native solution, so you will eventually be expected to migrate to a 5G Standalone solution. The section, “5G Non-Standalone (NSA) Deployments,” in Chapter', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 39, 'parent\_id': 'e8fc4656cc5607388f799c3b397f2bdf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e5cc0e210740e724c6835ac2e27100cd', 'text': '2, “Deployment Modes in 5G,” covers the different options of the NSA architecture in further detail.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 40, 'parent\_id': 'e8fc4656cc5607388f799c3b397f2bdf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd589e293b6d54a5895563ecd00b73f4b', 'text': '5G Standalone (SA) Solution', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 40, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f5261ac0af9048d6561ec359fe0f9a2', 'text': 'In Standalone (SA) architecture, the 5G Next-Generation Radio Access Network (NG-RAN), in conjunction with the 5G Core (5GC), is used for both the control plane and user plane, thereby removing any dependency on the 4G LTE Radio and Core network, as shown in Figure 1-7. This flexibility in deployment without any dependency on the 4G network and the openness from 5G Radio and Core allow industry verticals such as smart factories and healthcare to deploy private 5G infrastructures, also known as non-public networks (NPNs).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 40, 'parent\_id': 'd589e293b6d54a5895563ecd00b73f4b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aa21c559e28a3c094e8a809e780ab135', 'text': 'Figure 1-7 illustrates the 5G SA architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 40, 'parent\_id': 'd589e293b6d54a5895563ecd00b73f4b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'dfa255f92ea45acaf4fc303352398d8c', 'text': "= 5GC AMF / UPF (5G Packet Core) II i e T e e i .|---' 5G interfaces, examples: ; NG NG NG NG NN N, N - - Xn - - +— 9G Base Station", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 40, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da9a9f86e516b527671b58d122e97f7d', 'text': 'AMF - Access and Mobility Management Function UPF User Plane Function NGRAN - Next Generation Radio Access Network NG - Next Generation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 40, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '885050cc427b8431b6c72bf70d8673bb', 'text': 'AMF - Access and Mobility Management Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 40, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b093170a65eb9b1a3b148b77fe5be683', 'text': 'UPF User Plane Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 40, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '670aeadd9068bdbb36e389d42ba328d4', 'text': 'Figure 1-7 5G SA Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 40, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e234075b4ae71854fd4746eb93d8c8c0', 'text': '5G SA has several new capabilities, such as network slicing, CUPS, virtualization, automation, multi-Gbps support, ultra-low latency, and other such aspects that are natively built in to the 5G SA Packet Core architecture. Chapter 2 covers the SA architecture in more detail.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 41, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1011231c54923a0bd273e243c6ed638b', 'text': 'Service-Based Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 41, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd36c163bdabd956f5e31efbd141640c7', 'text': '5G SA introduces an all-new 5G Packet Core, as illustrated in Figure 1-8. 5G introduces service-based architecture (SBA), which is a framework defined by 3GPP that enables multivendor applications deployment and communications between them. In the SBA framework, the architecture elements are defined in terms of Network Functions (NFs) rather than by traditional Network Entities. Via interfaces of a common framework, any given NF offers its services to all the other authorized NFs and/or to any “consumers” that are permitted to make use of these provided services, thereby offering modularity and reusability.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 41, 'parent\_id': '1011231c54923a0bd273e243c6ed638b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '76fc98f03671c49700b4b986cb96cd89', 'text': "L L T L L O L e Lo T e D DO LOE G L e CY PEEL LR E LR L P T COECTCLIC R SBA Sewwce Based Architecture) 8Bl = EEEOE. - (Service Based Interface) Nudml Nnssf | Nnrf I Na i o o o API(HTTP JSON) Npcf I Nnef ' Namf ' N Nausf Network Functions smf SM = / ..-......-........-.. .-......-...... [ e ——— N1 ,’ N N4\\ === Control Plane ===~ DataPlane [ | — N6 3 Data Network / Internet b N9", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 42, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '4b485a3d6971c3d2a7f5d4acda2f5239', 'text': 'NSSF Network Slice Selection Function AMEF. - Access and Mobilty Management Function AUSF - Authentication Server Function UPF User Plang Function AF Application Function UoM Unffied Data Management SMF UE Session Management Function User Equipmen NEF Network Exposure Function SEPP Security Edge Protection Proxy NRF Network Resource Function ON Data Network nne Raliai Aanbeal £ aakia onn Qaniian Nammiininatian Dray', 'metadata': {'text\_as\_html': '<table><tbody><tr><td>AMF.</td><td>- Access and Mobilty Management Function</td><td>NSSF - Network Slice Selection Function</td></tr><tr><td>AF</td><td>Application Function</td><td>Uom - Unified Data Management</td></tr><tr><td>SMF</td><td>Session Management Function</td><td>User Equipment</td></tr><tr><td>NEF</td><td>Network Exposure Function</td><td>SEPP. - Security Edge Protection Proxy</td></tr><tr><td>NRF</td><td>Network Resource Function</td><td>Data Network</td></tr><tr><td>nnr</td><td>Naliai Nanbeal Fiinabinn</td><td>onn Qaniiaa Nammiininatian Drau</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 42, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e7a38c305dcd98db6edd92c0f7a033dd', 'text': 'Figure 1-8 5G Service Based Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 42, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bc8300b67c3114abe6a364c4ed8b030a', 'text': 'As shown in Figure 1-8, SBA is a control plane functionality using the application programming interface (API) with REST interface using HTTP/2, enabling different 5G network functions to exchange information within the 5GC control plane network functions. The SBA approach enables a fully distributed, fully redundant, stateless, and/or fully scalable deployment of 5G NFs. The capability to use APIs for communication and having the NFs fully virtualized allows 5G services to be provided from several locations, be it on- premises private cloud, public cloud, or hybrid cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 42, 'parent\_id': 'e7a38c305dcd98db6edd92c0f7a033dd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0628fe966971a5e5d323789ca5e92a56', 'text': 'Figure 1-9 illustrates the comparison of 4G and 5G control plane communications. API-based communication is now used for all 5G control plane communications instead of GTP-C and Diameter in 4G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 42, 'parent\_id': 'e7a38c305dcd98db6edd92c0f7a033dd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '1211edc6bde76d8305b8f6ccff2fefe7', 'text': '4G 5G - JSON GTP HTTP/2 UDP/TCP TLS IP TCP IP Diameter SCTP IP g S S —— e Secscccccm .-', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 43, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9d83b1eb882d6cf48b52b16a6acdb949', 'text': 'Figure 1-9 Comparison of 4G and 5G Control Plane Protocols', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 43, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b4297a08fdca0592c0c2758909de6149', 'text': 'The API is also used for exposing the capabilities of 5GC NFs with external third-party applications using the Network Exposure Function (NEF). This allows streamlining all communication between the 5GC and external third- party applications through the NEF. APIs are also extensively used in the orchestration and SDN deployments in 5G. The network slice as a service (NSaaS) offering will make use of API-based calls in the service layer for management access between the communication service provider (CSP) and communication service customer (CSC). Seeing the importance of APIs in 5G, 3GPP has also introduced Common API Framework (CAPIF) in Release 15, with enhancements in Release 16. The main purpose of CAPIF is to have a unified northbound API framework across several 3GPP functions. There is a single and harmonized approach for API development, with a number of 3GPP specifications in the works—to specify a framework to host APIs of PLMN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 43, 'parent\_id': '9d83b1eb882d6cf48b52b16a6acdb949', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6cfbd29e00ec38c7154ff12ba5c8afaa', 'text': 'and also to allow third parties to leverage the CAPIF framework to host their APIs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 44, 'parent\_id': '9d83b1eb882d6cf48b52b16a6acdb949', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '88016f2957bb1927401fc363da81f168', 'text': 'Adoption of Cloud-Native Technology', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 44, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a19687c230eba4f6a34e391977724ada', 'text': 'To achieve the economies of scale and enable new use cases that demand low latency and high scalability, 5G allows you to adopt cloud-native technologies to deploy 5G. Cloud-native is an approach to building and running applications that fully exploits the benefits of the cloud computing model. Adoption of cloud-native technology in 5G means that the network functions such as User Plane Function (UPF), Session Management Function (SMF), and so on can be built using open source software components and deployed on-prem or on a multistack public cloud as Cloud-Native Functions (CNFs), exploiting all the benefits of the cloud-native architecture. Here are some of the key benefits of cloud-native technology adoption in 5G:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 44, 'parent\_id': '88016f2957bb1927401fc363da81f168', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd65fdb2e9f6f7e092e28a3d754e70eda', 'text': '• Avoid vendor lock-in: The basic tenet of cloud-native architecture is based on open source and cloud technologies. All the 5G CNFs communicate using the API in the service-based interface (SBI) based on the service-based architecture (SBA). This makes it easier for you to select any vendor based on your criteria and then use the API for integration, thereby avoiding any vendor lock-in, including infrastructure- independent deployment of 5G CNFs on any hypervisor, bare metal or any public cloud provider.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 44, 'parent\_id': '88016f2957bb1927401fc363da81f168', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fca7877b367291c2271367a368039c4c', 'text': '• Scalability and resiliency: In 5G deployments, specifically for user plane CNFs like the User Plane Function (UPF), there will be the need to scale up and scale down based on capacity requirements due to a surge of traffic in a particular location. There is also a requirement for high availability in 5G to ensure service availability and prevent any downtime, as there might be revenue impacts and deployments related to national security. Auto scalability, high resiliency, and auto-provisioning are supported by cloud-native applications and network functions. Vulnerabilities can also be fixed faster, as cloud-native applications support DevOps process and automation, allowing you to patch the risks by deploying patched images quickly.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 44, 'parent\_id': '88016f2957bb1927401fc363da81f168', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '935a8ba5cd6e617b05198932e6d938aa', 'text': '• Orchestration: Virtualized 5G deployments in multi stack public cloud / multi-cloud and on-prem, along with the implementation of use cases such as network slice as a service (NSaaS), require end-to-end orchestration to', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 44, 'parent\_id': '88016f2957bb1927401fc363da81f168', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '203a951a488df96d2e94bddf53a2b5ff', 'text': 'ensure that all the related 5G CNFs have the right configuration to enable smooth running of the use cases without any need for manual intervention. Cloud-native technology such as Kubernetes ensures smooth automation of deployment, scaling, and management of containerized deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 45, 'parent\_id': '88016f2957bb1927401fc363da81f168', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ab50d861213930b01864494732d402b', 'text': 'A majority of the cloud-native technology projects are being handled by the Cloud-Native Computing Foundation (CNCF), which incubates the projects and brings them into fruition, which implies a level of technology maturity. One such example is Open Policy Agent (OPA), which is an open source, general-purpose policy engine that enables unified, context-aware policy enforcement across the entire stack and is integrated with other CNCF projects like Kubernetes, Envoy, CoreDNS, Helm, SPIFFE/SPIRE, and more. Projects with such integrations will allow you to have a consistent policy across your 5G CNFs, which are deployed across on-premises and multi stack public cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 45, 'parent\_id': '88016f2957bb1927401fc363da81f168', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4085eff5cf81128042c76ccb09beaf26', 'text': 'Multi-access Edge Computing (MEC)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 45, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6f50b9939398969f2df343a2f3009c27', 'text': 'Multi-access edge computing (MEC) is acknowledged as one of the key pillars for meeting the demanding key performance indicators (KPIs) of 5G, especially as far as low latency and bandwidth efficiency are concerned. Edge computing as an evolution of cloud computing brings 5G network functions and applications from centralized data centers down to the network edge, closer to consumers and the data generated by devices and applications. However, not only is edge computing in telecommunications networks a technical enabler for the demanding KPIs, it also plays an essential role in the transformation of the telecommunications business, where telecommunications networks are turning into versatile service platforms for industry and other specific customer segments. This transformation is supported by edge computing, as it opens the network edge for applications and services, including those from third parties. MEC provides a new ecosystem and value chain by enabling third-party application developers and the cloud-computing capabilities of content providers, as well as an IT service environment at the edge of the network. Operators can open their Radio Access Network (RAN) edge to authorized third parties, allowing them to flexibly and rapidly deploy innovative applications and services toward mobile subscribers, enterprises, and vertical segments. Depending on your network design, MEC applications and user plane functions could be set up on private cloud, public cloud, or hybrid deployments, enabling ultra-low latency and high bandwidth as well as real- time access to radio network information that can be leveraged by applications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 45, 'parent\_id': '4085eff5cf81128042c76ccb09beaf26', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5875d5ed60dfa93915f683f90e6a9170', 'text': 'The European Telecommunications Standards Institute (ETSI) MEC framework, as illustrated in Figure 1-10, provides an architecture reference to create a standardized, open environment that allows the efficient and seamless integration of applications from vendors, service providers, and third parties across multivendor MEC platforms.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 46, 'parent\_id': '4085eff5cf81128042c76ccb09beaf26', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ff1d781348321ecb59353cd0a077a47c', 'text': 'Mt Operations MEC Mm8 i Support System Device M2 User app system pp LCM proxy Mimt level Mm9 MEC i Orchestratpr e a3 1 3 T T ryeer Mm2 Mm3 Mmd Other Mp3 MEC Service MEC MEC MEC app MEC app platform Platform rules and Ifecycle MEC bt = element host reqfs manage- level manager manager ment Traffic ONS Tules Handl- MEC platform manager MEE : control ing MEC Platform Mm6 Other Mp2 J MEC host Virtualization Infrastructure Mm? MEC Host MEC: Mult-Access Edge Compute CFS: Customer Facing Service', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 46, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b1c8821b4093c1b7e9c8a768accd5915', 'text': 'MEC: Mult-Access Edge Compute', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 46, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b95d4268255706fc8d440b786af4972f', 'text': 'CFS: Customer Facing Service', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 46, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1c04291877f93a7543be4bfb7b0ba12e', 'text': 'Figure 1-10 ETSI MEC Framework', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 46, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '78cc17bfb28b6e0ff0e1a07646c05eb0', 'text': 'The key components of the MEC architecture framework, as shown in Figure 1-10, are discussed in detail next.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 46, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '721d8f01fff9ec0e65665df5fb0ef9c7', 'text': 'The MEC host level provides compute, storage, and network resources for the MEC applications, which includes a data plane that executes the traffic rules received by the MEC platform, and routes the traffic among applications, services, DNS server/proxy, 3GPP network, other access networks, local networks, and external networks. The core entities of the MEC host level are composed of the MEC platform (MEP), applications, UPF data plane, MEC platform manager (MEPM), and virtualization infrastructure. The MEPM is responsible for managing the MEP.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 47, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '804c1c642e910b347e34fea31d7e9638', 'text': 'MEC system-level core entities are composed of the MEC orchestrator, which helps in on-boarding of application packages, including checking the integrity and authenticity of the packages, validating application rules and requirements, and maintaining an overall view of the MEC system.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 47, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3de26481aa76b5f29eccfbdd177e0276', 'text': 'To avoid duplication and inconsistency of approach between different API specifications, 3GPP has considered the development of a common API framework for 3GPP northbound APIs (CAPIF) that includes common aspects applicable to any northbound service APIs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 47, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '103b8b0a69d62d1c2aea9a39cb704573', 'text': 'Network Slicing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 47, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3a6f823968c59eef54737d6216cf4527', 'text': '5G SA provides flexibility and openness for service providers to serve vertical use cases by peeling off a part of your network and offering it to the industry verticals with a network slicing feature that provides you with the right level of isolation, ease of management, and service level agreements (SLAs). This type of service offering is called network slice as a service (NSaaS). The type of private 5G network that integrates with service providers is called the public network integrated non-public network (PNI-NPN). Private networks can use the licensed, unlicensed, dedicated, and shared spectrum with other service providers. Deploying 5G in the industry verticals drives tremendous gains in productivity, economic growth, and other benefits.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 47, 'parent\_id': '103b8b0a69d62d1c2aea9a39cb704573', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1e1938e0b5678d3b5b72e5f1b4e16eaf', 'text': 'A network slice can be seen as a logical network serving a defined business purpose or customer, consisting of all required network resources configured together. Network slicing divides your physical network into multiple logical networks or domains. These logical networks/domains would permit the implementation of tailor-made functionality and network operation specific to the needs of each slice customer, rather than a one-size-fits-all approach, as witnessed in the current and previous mobile generations.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 47, 'parent\_id': '103b8b0a69d62d1c2aea9a39cb704573', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cb5f8abce99b073f7153ba9d3fe6e5a2', 'text': 'The network slicing domains can consist of Radio Access Network (RAN), Transport Network, 5G Core (5GC) Network Functions, and also third-party applications. Some of the domains can overlap multiple slices; for example, certain 5GC network functions such as the Network Slice Selection Function (NSSF) and Policy Control Function (PCF) can be shared between multiple slices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 48, 'parent\_id': '103b8b0a69d62d1c2aea9a39cb704573', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e416e47fd6fbae40181af9fbc0dae8a3', 'text': 'As shown in Figure 1-11, successful implementation of a network slice requires network slice member management, configuration of slice SLAs and quality of service (QoS), a multidomain software-defined network (SDN),and end-to-end orchestration. Without the capability of end-to-end slice management with end-to-end domain components, implementation of a successful network slice would be nearly impossible and extremely difficult to manage and operate.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 48, 'parent\_id': '103b8b0a69d62d1c2aea9a39cb704573', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a7b4a0f5573e189381499da46cc78a95', 'text': 'Figure 1-11 illustrates the example of multiple domains in a network slice implementation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 48, 'parent\_id': '103b8b0a69d62d1c2aea9a39cb704573', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '75d7fc3ebc49d36494c004b2d911f330', 'text': 'LT T T T T L L Service Layer canin \\ Senvice Provider \* Domain or external E—— e 4 f Mult-Domain SDN and Orchestration layer sssssssnesssssnssssesssansssnaans ( Slice 1 56C —— i om o l E DT oD SRy SRRy Uy EpEpppRpppRpspppay ! Slce? 39Pa ry oo pplicati =3 n oo TooT T oTooTooeeY i T e e e A e e e e ) UE : User Equipment NG-RAN: Next Generation Radio Access Network 5GC : 5G Packet Core QoS : Qualty of Senvice SLA: Senvice Level Agreements SON : Software Defined Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 49, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '928cd2ee70de0a3cee5b2680640aa873', 'text': 'UE : User Equipment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 49, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '52693c99d6195899ba26d85e2930367b', 'text': 'NG-RAN: Next Generation Radio Access Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 49, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '544ec80500c1f835afda9d99144f3e8a', 'text': '5GC : 5G Packet Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 49, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7ae5c5afa50d50ffa4633b969c6367de', 'text': 'QoS : Qualty of Senvice', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 49, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '04900c628fd134e0f88b100d0371c445', 'text': 'SLA: Senvice Level Agreements', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 49, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4c3ee7d7b892cbf7d563bf4d41a8aa20', 'text': 'SON : Software Defined Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 49, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8e4c509bc269acfccb3bfdf8da6aac7a', 'text': 'Figure 1-11 Multiple Domains Within a Network Slice Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 49, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6f6c2f4d2f74aa933a60ccd85ff5762c', 'text': 'Chapter 7, “Securing Network Slice, SDN and Orchestration in 5G,” covers the topic of network slicing, its threat surface, and mitigations in more detail. The section “Private 5G/Non-Public Networks” in Chapter 2, “Deployment Modes in 5G,” covers the topic of network slicing deployment modes for the non- public network (NPN) and public network integrated non-public network (PNI- NPN) in more detail.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 49, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'text': 'Key 5G Features in 3GPP Releases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 49, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1760349853ae343e4d4b8c35f10a94fe', 'text': 'This section discusses the key 5G features in Releases 15, 16, and 17. The overall trend in Release 16 onward is to make the 3GPP 5G System (5GS) more open and more of an enabling platform for industry verticals such as smart factories, transportation industry, and healthcare. The features in present and future releases, as illustrated in Figure 1-12, are geared to improving the adaptability of 5G toward non-3GPP industrial networks with enhancements in URLLC, network slicing, MEC, cellular IoT (C-IoT), secure communication based on APIs with third-party Application Functions (AFs), non-public networks, positioning services, and LAN-type services.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 50, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b8aa0952202d6a7a44793fdf40e15497', 'text': 'Figure 1-12 lists the key features for 5G in 3GPP Releases 15 and 16 and the key the features planned for Rel-17.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 50, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '05b1536e0d64cb38db7116a89940e2d3', 'text': '5G Phase 1', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '25f2bbc1e7b6029760ea4a9c0e5f170f', 'text': '5G Phase 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8f803627dfe43066d296e37fa36f27e3', 'text': 'Release 15', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c8ac81cc893b6c70e781cb098e13c57b', 'text': 'Release 16', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a9563be98fcb64ff7ab34c051ccbd6b2', 'text': '(2017-2019)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '890f2c61c47123daf28a4a0a64c845fd', 'text': '(2018-2020)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0c07a337396f62f9a326d4ca728ddf96', 'text': '56 System & Packet Core:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '93d74405d032ad6b04526b78d6f2f968', 'text': '5G System & Packet Core:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'a33c3babf0683013631894b10834f5d5', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f4b6f50f9694f6ef0b1c80a52d60218b', 'text': 'SBA based architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'ListItem', 'element\_id': 'cd8978604c31f744fc3a6ab5eb36c19a', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c4c4a36fb5bae2025cd672a956561465', 'text': 'Anchored NR-U', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'c004536fd7b1e1cd8b86602e15a65537', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd1f69a2eacd7ce3da24b6428abcc8abe', 'text': 'Massive MTC & loT', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '56996f8471f9bea057abaeba917c78f9', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36a2d6818f9cd1d112e98f248c832c25', 'text': 'Standalone NR-U', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '9cb7e43b0f47dff0be094babbd9777ab', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '3bfe96caf8e01860e96d459920e98fdf', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd8e225398d5b36b6704eddcdf2964e82', 'text': 'API Exposure to 3¢ party', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '98cf4c30961c62e64086655c131ecb29', 'text': 'Cloud friendly (SBI)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'ListItem', 'element\_id': '033fb7c2fc5dd2d447c2f2fcaefdaedc', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '01309cfe94b1efa191a7918c2b632a0a', 'text': 'Integrated Access & Backhaul (1AB)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '190fe68eb6553e9f6e9b72db5a946d91', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6419bb36e58801b5f1047dd2baf2709e', 'text': 'Network Slice as a Service', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '9a5117abaf36a4bb11e3ea3772b87f9c', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b2846e8fcc2e8959c07af1c1031c2f0d', 'text': 'CAPIF enhanced', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '5b2b63b133143b847207a92ffb138f5c', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e445a4ffdddb30e8258c5a4a7cc8496c', 'text': 'EC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a5a1706cf7f0e61ec1e3e38453767c24', 'text': 'RAN:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '15f0b20c8bf688a12bea36cacff5ac10', 'text': 'RAN:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'b0cdb8dd1b86f4e9afac06cfb36a1f8c', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '403afdae78585738324cd4d066f10bae', 'text': 'NR Positioning', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'bdcdb87cc7e3dd9efa5050076de4425c', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '39070a91ed5464682cb92f709cfaa9db', 'text': 'New Radio specification', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'a0afbed1d278d20dc9c7eaec05b89ead', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '187b922904337314e2daa61cbc232b96', 'text': 'NR Coverage', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '7c81dae85195f9380c92a7b51345900c', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e28a2745e20c0b3a5b8198e062b119a5', 'text': 'NRNSA (option 3x)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'b0498dea2b2ed18e18add28f4a3b3ad6', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2c3a8fc5eb74a4d04675ae21b099e21f', 'text': 'UE power saving techniques', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '539cdf9614522a5fe33ee82dd2158d16', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ead1b2013489c4b119cf122065026580', 'text': 'NR S opion 264/57)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '45643fc1e9f9f13c7363e722b66a9440', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b758604874ee80cfca89574b90cd1d9e', 'text': 'HARQ enhancement', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'b33677251c1a5df851e13ced7cf9f262', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ac8aee6ca1182c0703f15b29ecabf2b8', 'text': 'Wide bandwidth (~400 MHz)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '83bf67d9b419c037dc66d3b4a8ba6d05', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6fe550c0604de98f68d0d1c4c7606560', 'text': 'Enhanced Scheduling', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '181e282ee89a512ffdb4993372570475', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36cb3bd082da79804933edcfc42658ec', 'text': 'Wide Freq Range (upto 28GHz', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '516b42c9a9d50509ba0175782236bfb1', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f0c3027e75f23966df7ca900fcda628d', 'text': 'Coordinated multi-point (CoMP)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'be4912786f1dcd2ce5fc110da400a0ef', 'text': 'Industry verticals:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f664a9c1be9045beb5be4bc1519fb293', 'text': 'Industry verticals:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '66c849cd5b82558a771048ae56265365', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2ab70de021162e8ed275159a362f139d', 'text': 'V2XPhase 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'deea5dfb089fb8a72ebf9b23008ab488', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '92ed6b4902bc9e1795dda5385f1afd65', 'text': 'Time Sensitive Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '6e726f4213ffe1eda7bf6c9f515f5876', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f75c8a3401ae82c4ced1344c48875cb1', 'text': 'Mission Critical Interworking', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'de38698209dfa4d22e9ef42577befaec', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c11031648cc9641d6e3410d911746c1e', 'text': 'C-V2X enhancement', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'e482ed2517db0aa83c5a39f655881d34', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58e1dd6a9a8d22fd26cc1a140c1d03b9', 'text': 'WLAN and unlicensed spectrum', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '3f494dbbf6ae4d6ed4046d6cfe1f35b1', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aeb55322573d574cc69d456d9adc4497', 'text': 'lloT & URLLC support', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '919db8748eea68ad0443a1cf132fe09e', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2fe42f15116cb32c44f61f1c12d084c', 'text': 'NPN support', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'e9adb3bd4f970353400805d61c1a68a1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0dc09593178287a587671db1f489bf13', 'text': 'www.3GPP.org/specifications/work-plan', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '54ce4531cf51d42c47fbcf5a1176390e', 'text': 'Phase 3 Release 17 (2020-2022 expected)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '077ea52569885b05e5210a45aa00c36b', 'text': '5G System & Packet Core:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '5a8c397e5ae13fcb35a8e50ce0c24e06', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1bb0652dbc60861ebe097f47a27b8510', 'text': '5G LAN type services', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'ListItem', 'element\_id': 'f63352856ac1a3777b8ae4503f057bf2', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58397f59bc00f764e024ee7e90e3c811', 'text': '5G Wireline & Wireless Convergence', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'ListItem', 'element\_id': 'd1c733f0bf48c63e293df715ab1ca9cb', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0f6dde5dd803ffa77cdfc9c3fe26ea0d', 'text': 'Edge Computing in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'ListItem', 'element\_id': '3b489a2a77db2a7790742f04dfc7b240', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1f42fe513116b6a41a59f3141ed78b8a', 'text': '|AB enhancement', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'ListItem', 'element\_id': '2c4afd5ba22412c73003c809076727e1', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2a344400500c0f98686ce3c1ec7a8ad', 'text': 'Network Slicing - phase 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'ListItem', 'element\_id': '432b613149eed1e1646939088772678e', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'edb7c2e9b7a4b6469385c242e8596c42', 'text': 'Multi-SIM', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'ListItem', 'element\_id': '35523f8fa13015762e63d6141e1dd163', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fcb820d26a128c7607e413614866c5ba', 'text': 'Access Traffic Steering', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6d8722ff32a1a4c4125c55ca3746be8d', 'text': 'RAN:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'ListItem', 'element\_id': '679a915f4cd8997977f7752ade9f7705', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c6ebb29fae3285b583f6a9687d3a548f', 'text': 'NR Coverage enhancement', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'ad2aae5261bf69e01b2e6d32d86bd54c', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8a61159411bdc7aa68ff551915b2336c', 'text': 'NR Positioning enhancement', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '1c06b0d6a441516bb5761fbac3fe5b3f', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1161bd1c27ee0a50f8193d921fa50258', 'text': 'NR Quality of Experience', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'dd510a5464abe2829f6bff46205ec90f', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da5cd3f89630d310368b868a7fe4de2b', 'text': 'NR MIMO', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '077da4e89dd14da0b103ad543ac78f1b', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5a4c67b6b632df464c48e94c225edd61', 'text': 'RAN Slicing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '6cbef75651140c21e88ebf629dd2735f', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2ab234cd4213c869676ea5625680d90f', 'text': 'Mutti-Radio DCCA enhanced', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'efc2859c8cf84971b15a456984385a71', 'text': 'Industry verticals:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '452ca99091e0cdfed0f3e1168fff9703', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '639321821eb06548a504072ad0ef9fba', 'text': '[loT & URLLC enhanced', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'd0a032bdcf41f3ffc180d36440923563', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c68c38e24225747c8e13d8b28d7d0f12', 'text': 'NB-loT & LTE-MTC enhancement', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '2b2dd94af41986a335fe33de6820a479', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '506ec2119cec14c148a4a52b0a9d30ee', 'text': 'Unmanned Aerial Systems', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'efd739fee2a4d549fbbddb900566caad', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e174be4af431e156217ed8b6646d0260', 'text': 'Satellite components', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '2d19abcaf4a85f86e90315bf73dcf675', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '091d28ff149fb974016d2110bea337fc', 'text': 'Enhanced V2X Services', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '73f0d871562fea7261c377ef67012e75', 'text': '.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f05b07ed6de182455a4e1447051ce883', 'text': 'NPN enhanced', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': '0dc09593178287a587671db1f489bf13', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b03116a1a525e00cb8d84084a6f201f2', 'text': 'SBA', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '367e982e15230b9067c0499ed1e9d0d0', 'text': 'WLAN: Wireless Local Area Network : Service Based Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'b03116a1a525e00cb8d84084a6f201f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd289d5afe818dae51b054a93bf9c20d6', 'text': 'Figure 1-12 Key 5G Features in 3GPP Release 15, 16, and 17', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 51, 'parent\_id': 'b03116a1a525e00cb8d84084a6f201f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ebd10b660faef361344be6fb8c96252', 'text': 'In 3GPP Release 16 (Rel-16), the key areas of enhancements in APIs are toward aligning northbound APIs with the Common API Framework (CAPIF), as defined in 3GPP TS 29.222, where the following are introduced:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 52, 'parent\_id': 'b03116a1a525e00cb8d84084a6f201f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0d36c9de540d713a93470711a89f16a1', 'text': '• Enhanced event report to support detailed event reporting of CAPIF events', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 52, 'parent\_id': 'b03116a1a525e00cb8d84084a6f201f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7c85067af7bf0df368442ec6481da83b', 'text': '• Network Exposure Function (NEF)/Services Capability Exposure Function (SCEF) Northbound (NB) API registration with CAPIF Core Function to enable discovery of the NB APIs by external Application Functions (AFs)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 52, 'parent\_id': 'b03116a1a525e00cb8d84084a6f201f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '51c9805efe4c09e1b025434819735b8a', 'text': '• Defining the Uniform Resource Identifier (URI) structure for APIs related to N33 and T8 interfaces', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 52, 'parent\_id': 'b03116a1a525e00cb8d84084a6f201f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9bdb3a86f525c07ac9022639a34704a5', 'text': 'While a basic Common API Framework is made available in 3GPP Rel-15, there are several enhancements that are considered for eCAPIF in Rel-16 to enable the API exposing function, the API publishing function, and the API management function of the API provider domain within the third-party trust domain interaction with the CAPIF core function in the PLMN trust domain.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 52, 'parent\_id': 'b03116a1a525e00cb8d84084a6f201f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e10991c6fbbcf94489c42630777af6f4', 'text': 'The main purpose of CAPIF is to have a unified northbound API framework across several 3GPP functions. There is a single and harmonized approach for API development, with a number of 3GPP specifications in the works—to specify a framework to host APIs of the PLMN and also to allow for third parties to leverage CAPIF to host their APIs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 52, 'parent\_id': 'b03116a1a525e00cb8d84084a6f201f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd2182cad767a53b8528c339cb07bdd52', 'text': 'Key 5G Advanced Features', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 52, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '317c673f6d5c64e2114bde2cec0f4804', 'text': 'This section discusses the key 5G features, which are under study in 3GPP Release 18. 5G naming conventions will evolve to 5G-Advanced with the forthcoming Release 18 from 3GPP. Figure 1-13 illustrates the key features under study for 5G Advanced.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 52, 'parent\_id': 'd2182cad767a53b8528c339cb07bdd52', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f47b2e69de69fe8d356905943c7c7703', 'text': 'placeholder', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 53, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a5ec38f579a358b80418be1cc50209f', 'text': 'Figure 1-13 Key 5G Advanced Features under study in 3GPP Release 18', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 53, 'parent\_id': 'f47b2e69de69fe8d356905943c7c7703', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '57b91810d977f0933633008e3203fd7d', 'text': 'In 3GPP Release 18 (Rel-18), the key areas of enhancements are related to immediate and longer-term commercial needs for the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 53, 'parent\_id': 'f47b2e69de69fe8d356905943c7c7703', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3b735d7527679b5b44f7f27dd550f5b4', 'text': '• Evolved Mobile BroadBand (eMBB)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 53, 'parent\_id': 'f47b2e69de69fe8d356905943c7c7703', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd825716ecebfdafba70ff23bcdb0bc7c', 'text': '• Non-eMBB evolution', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 53, 'parent\_id': 'f47b2e69de69fe8d356905943c7c7703', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '799ee618f9fb8cf58996203b63b2fb5c', 'text': '• Cross functionalities for both eMBB and non-eMBB driven evolution', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 53, 'parent\_id': 'f47b2e69de69fe8d356905943c7c7703', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1fcc50189d675642207f08683c964f21', 'text': 'Majority of the enhancements under study in Rel-18 is aimed at getting improved data throughput rates in uplink (UL); improvements in getting lower latency and higher bandwidth for gaming and eXtented Reality (XR); and enhancements to allow seamless deployments of Non-Public Network deployments. As per the 3GPP work plan proposal, Rel-18 is expected to be ready by December 2023.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 53, 'parent\_id': 'f47b2e69de69fe8d356905943c7c7703', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '38241753c93001e1fa6b2d7b02426acc', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 53, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2ba4b5d4a20dd77da4bccb505fd5c595', 'text': 'As discussed in this chapter, the earlier generations of cellular technology such as 4G focused on ensuring connectivity, whereas 5G takes connectivity to the next level by delivering connected experiences from the cloud to clients. Even antenna technologies will see increased adoption of MIMO and algorithms to enhance beamforming based on the density of users and type of application. This is a major shift from passive antenna technologies such as panel antennas with just remote down-tilts and up-tilts. 5G technology uses a new spectrum but is not limited to it. 5G is designed to support a converged, heterogeneous', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 53, 'parent\_id': '38241753c93001e1fa6b2d7b02426acc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '89a1f88633e41cb2d7440aca933e005a', 'text': 'network, combining licensed and unlicensed wireless technologies. This will add bandwidth available for users and devices being catered for by 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 54, 'parent\_id': '38241753c93001e1fa6b2d7b02426acc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d47dbd25cd9f1305e2b2912b59557b6', 'text': '5G networks are virtualized and software driven, with open, flexible deployment models, and they exploit cloud technologies and software-defined platforms, in which networking functionality is managed through software rather than hardware. Advancements in virtualization, cloud-based technologies, adoption of APIs, IT, and business process automation enable 5G architecture to be agile and flexible and to provide anytime, anywhere user access. 5G networks can create software-defined subnetwork constructs known as network slices, which enable you to create an isolated end-to-end network consisting of both virtualized and physical components tailored using automated provisioning and proactive management of traffic and services to fulfill diverse requirements requested for a particular application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 54, 'parent\_id': '38241753c93001e1fa6b2d7b02426acc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e25e72e093d7c66e834787d8407bcbb', 'text': 'Although Rel-17 5G and Rel-18 5G is looking at enhanced capabilities and evolution of features for MIMO, NPN, and better security in API communications, it has to be noted that there is usually a 2-to-3-year delay in the features, which has impacts on radio access network (RAN) and user devices (UE). Being pragmatic, real-world deployments of 5G standalone (SA) will be around at the end of 2022 and the beginning of 2023. For Rel-17, the deployments are expected to be around 2024 and Rel-18 around 2025-2026.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 54, 'parent\_id': '38241753c93001e1fa6b2d7b02426acc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c5f713b95b3306ab9921d29d86d2598a', 'text': 'Acronym Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 54, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '37ccbd7ff9a6a88a7be1f2433bd5cd56', 'text': 'The following table expands the key acronyms used in this chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 54, 'parent\_id': 'c5f713b95b3306ab9921d29d86d2598a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '155d2b2eeb9d03f9709f3929c7d746df', 'text': 'Acronym Expansion 5GC 5G Core network AKA Authentication and key agreement API Application programming interface BH Back haul DAPS Dual Active Protocol Stack eMBB Enhanced mobile broadband eNB E-UTRAN NodeB EPC Evolved Packet Core FH Front haul New Radio NodeB gNB GTP GPRS Tunnelling Protocol HAPS High Altitude Platform System HTTP Hypertext Transfer Protocol HW Hardware IAB Integrated access and back haul T Industry Internet of Things IoT Internet of Things IP Internet Protocol', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Acronym</th><th>Expansion</th></tr></thead><tbody><tr><td>5GC</td><td>5G Core network</td></tr><tr><td>AKA</td><td>Authentication and key agreement</td></tr><tr><td>API</td><td>Application programming interface</td></tr><tr><td>BH</td><td>Back haul</td></tr><tr><td>DAPS</td><td>Dual Active Protocol Stack</td></tr><tr><td>eMBB</td><td>Enhanced mobile broadband</td></tr><tr><td>eNB</td><td>E-UTRAN NodeB</td></tr><tr><td>EPC</td><td>Evolved Packet Core</td></tr><tr><td>FH</td><td>Front haul</td></tr><tr><td>gNB</td><td>New Radio NodeB</td></tr><tr><td>GTP</td><td>GPRS Tunnelling Protocol</td></tr><tr><td>HAPS</td><td>High Altitude Platform System</td></tr><tr><td>HTTP</td><td>Hypertext Transfer Protocol</td></tr><tr><td>HW</td><td>Hardware</td></tr><tr><td>IAB</td><td>Integrated access and back haul</td></tr><tr><td>T</td><td>Industry Internet of Things</td></tr><tr><td>IoT</td><td>Internet of Things</td></tr><tr><td>IP</td><td>Internet Protocol</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 55, 'parent\_id': 'c5f713b95b3306ab9921d29d86d2598a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '39f1b6bd5537e3607f57948c05d1e221', 'text': 'IR Incident response IT Information technology JSON JavaScript Object Notation KPI Key performance indicators M2M Machine-to-machine MBB Mobile broadband MBS Multicast Broadcast Service MEC Multi-access edge compute MDT Minimization of Drive Test MH Mid haul MitM Man in the middle MIMO Multiple Input Multiple Output NGAP NG Application Protocol NID Network identifier NPN Non-public network NR New Radio PLMN Public land mobile network PNI-NPN Public network integrated NPN QAM Quadrature amplitude modulation RNC Radio network controller S-GW Serving gateway SCTP Stream Control Transmission Protocol SFC Service Functionality Chaining', 'metadata': {'text\_as\_html': '<table><thead><tr><th>IR</th><th>Incident response</th></tr></thead><tbody><tr><td>IT</td><td>Information technology</td></tr><tr><td>JSON</td><td>JavaScript Object Notation</td></tr><tr><td>KPI</td><td>Key performance indicators</td></tr><tr><td>M2M</td><td>Machine-to-machine</td></tr><tr><td>MBB</td><td>Mobile broadband</td></tr><tr><td>MBS</td><td>Multicast Broadcast Service</td></tr><tr><td>MEC</td><td>Multi-access edge compute</td></tr><tr><td>MDT</td><td>Minimization of Drive Test</td></tr><tr><td>MH</td><td>Mid haul</td></tr><tr><td>MitM</td><td>Man in the middle</td></tr><tr><td>MIMO</td><td>Multiple Input Multiple Output</td></tr><tr><td>NGAP</td><td>NG Application Protocol</td></tr><tr><td>NID</td><td>Network identifier</td></tr><tr><td>NPN</td><td>Non-public network</td></tr><tr><td>NR</td><td>New Radio</td></tr><tr><td>PLMN</td><td>Public land mobile network</td></tr><tr><td>PNI-NPN</td><td>Public network integrated NPN</td></tr><tr><td>QAM</td><td>Quadrature amplitude modulation</td></tr><tr><td>RNC</td><td>Radio network controller</td></tr><tr><td>S-GW</td><td>Serving gateway</td></tr><tr><td>SCTP</td><td>Stream Control Transmission Protocol</td></tr><tr><td>SFC</td><td>Service Functionality Chaining</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 56, 'parent\_id': 'c5f713b95b3306ab9921d29d86d2598a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '71275de4ec948b91590ae6e9d57384f2', 'text': 'SNPN Standalone Non-Public Network SON Self Organizing Networks TLS Transport Layer Security UAV Unmanned Aerial Vehicle UE User equipment UPF User Plane Function URLLC Ultra-reliable and low-latency communications V2I Vehicle-to-infrastructure V2N Vehicle-to-network V2P Vehicle-to-pedestrian Vv Vehicle-to-vehicle V2X Vehicle-to-everything WLAN Wireless local area network X2 GW X2 gateway X2-C X2-control plane X2-U X2-user plane Xn-C Xn—control plane Xn-U Xn-user plane XnAP Xn Application Protocol XR eXtended Reality', 'metadata': {'text\_as\_html': '<table><thead><tr><th>SNPN</th><th>Standalone Non-Public Network</th></tr></thead><tbody><tr><td>SON</td><td>Self Organizing Networks</td></tr><tr><td>TLS</td><td>Transport Layer Security</td></tr><tr><td>UAV</td><td>Unmanned Aerial Vehicle</td></tr><tr><td>UE</td><td>User equipment</td></tr><tr><td>UPF</td><td>User Plane Function</td></tr><tr><td>URLLC</td><td>Ultra-reliable and low-latency communications</td></tr><tr><td>V2I</td><td>Vehicle-to-infrastructure</td></tr><tr><td>V2N</td><td>Vehicle-to-network</td></tr><tr><td>V2P</td><td>Vehicle-to-pedestrian</td></tr><tr><td>Vv</td><td>Vehicle-to-vehicle</td></tr><tr><td>V2X</td><td>Vehicle-to-everything</td></tr><tr><td>WLAN</td><td>Wireless local area network</td></tr><tr><td>X2 GW</td><td>X2 gateway</td></tr><tr><td>X2-C</td><td>X2-control plane</td></tr><tr><td>X2-U</td><td>X2-user plane</td></tr><tr><td>Xn-C</td><td>Xn—control plane</td></tr><tr><td>Xn-U</td><td>Xn-user plane</td></tr><tr><td>XnAP</td><td>Xn Application Protocol</td></tr><tr><td>XR</td><td>eXtended Reality</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 57, 'parent\_id': 'c5f713b95b3306ab9921d29d86d2598a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '131cb33c5538b792c74235c57bcd2c4a', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 57, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'de5e5d723083980c846684e4833df3d2', 'text': 'Pramod Nair, “Securing Your 5G Infrastructure to the Edge and Beyond,” Cisco Public, April 1, 2021', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 57, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4ffdd1a98bdf7eb16efbcf449f874cca', 'text': 'Pramod Nair, “Securing 5G and Evolving Architectures,” Cisco Knowledge Networks, Cisco Public, September 17, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '84dc9482cf084674500a74a57a527ea5', 'text': 'ETSI GS MEC 003, “Multi-Access Edge Computing (MEC): Framework and Reference Architecture”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '037a70a06ab572ab5de9813e7a4d9d02', 'text': 'Framework and Reference Architecture”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f48df46c2520eddea15f4b091ea0aaa1', 'text': '3GPP work program, https://www.3gpp.org', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '39d522246918693cde7cc723798b7e3b', 'text': '3GPP TS 23.501, “System Architecture for the 5G System: Stage 2”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0a82cc028c8743db5b6c405c686297d5', 'text': '3GPP TS 38.401, “NG-RAN: Architecture Description”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '677b1a62b1aea142152b1bee7f12d2f0', 'text': '3GPP TS 33.501, “Security Architecture and Procedures for 5G System”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '94047b8e16d4fe10c1e1a583e5056b4a', 'text': '3GPP TS 29.122, “T8 Reference Point for Northbound Application Programming Interfaces (APIs)”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d54ff525a6aa01176faad8176f9863b', 'text': '3GPP TS 38.470, “NG-RAN: F1 Application Protocol (F1AP)”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '603960b8b18a944b2ba1805f1e414287', 'text': '3GPP TS 38.300, “NR: NR and NG-RAN Overall Description”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '74db7dcb9406f2c0f944388de9b9c4b9', 'text': '3GPP TR 21.915, “Release 15 Description: Summary of Rel-15 Work Items”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '77467ce3ea1073e3e9bec6a9f12f8bc5', 'text': '3GPP TR 21.916, “Release 16 Description: Summary of Rel-16 Work Items”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '78dd93fd5fefdf03185dfa0d7373b489', 'text': 'TS 29.222, “Common API Framework for 3GPP Northbound APIs” TS 29.522, “5G System: Network Exposure Function Northbound APIs: Stage 3”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bf0c921ca89688452b0c60afd8e4be6c', 'text': '3GPP TS 36.101, “Evolved Universal Terrestrial Radio Access (E- UTRA): User Equipment (UE) Radio Transmission and Reception”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '083c6bbd9f73509c03cf3d98a3085bfe', 'text': 'Cisco Systems, “Reimagining End-to-End Network Mobile Network in the 5G Era,” Cisco Public, 2019', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 58, 'parent\_id': '131cb33c5538b792c74235c57bcd2c4a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e6715184a541eb2a95d23f12501bc856', 'text': 'Chapter 2. Deployment Modes in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 59, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a9386c04f85b4bb793a144f1a0517510', 'text': 'After reading this chapter, you should have a better understanding of the following topics:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 59, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '161428e92cda06dd4bdeef841a96220a', 'text': '• Multiple 5G SA and NSA deployment options', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 59, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '47cf33e6b1b5839553875bee1f1d1b1a', 'text': '• Public and non-public network deployment models in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 59, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd33afeff86629943a82fc6570e19fde5', 'text': '• Interworking between 4G and 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 59, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eee6b6bd34d59cadaea1b35ab9f323fe', 'text': '• 5G LAN type deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 59, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fe23774eeb817d25dde511911b72285f', 'text': 'The previous chapter took you through the evolution of cellular technologies— in particular, the evolution of cellular technology from 4G to 5G. This chapter takes you through the different modes of 5G deployment and the use cases that can be mapped to deployment modes.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 59, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0bb94813da327d125f4bc1b90198266a', 'text': 'This chapter should be of particular interest to the following individuals and teams from enterprise/5G service providers deploying 5GC and cybersecurity vendors planning product developments for 5G security use cases:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 59, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ec3cdf925d30d249c94b60d8c334288a', 'text': '• Security leaders within government organizations who would like an understanding of 5G deployment modes', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 59, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3c6e2b69c2a827e94563f459346fea7b', 'text': '• Teams from enterprise and industry verticals that want an understanding of 5G deployment modes', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 59, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ee5cb2787691317001816c0900de856d', 'text': '• Enterprise cybersecurity vendor security architects looking to have an understanding of 5G deployment modes', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 59, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1bb9aa393f56df97cb9feca2183bd045', 'text': '• Cybersecurity students who would like to get a brief understanding of 5G deployment methods', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 59, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3abee97e1f1fc22c28ac882c0500ca77', 'text': '5G brings in real openness and deployment flexibility, with many options to choose from. Service providers who have already invested billions in network infrastructure in 2G, 3G, and 4G technologies can reuse parts of the 4G infrastructure for initial deployment of 5G. Such deployments are called 5G Non-Standalone (NSA). 5G also introduces deployment options where all the components of 5G System (5GS) are purely 5G and have no dependencies on 4G and legacy cellular technologies. Such deployments are called 5G Standalone (SA).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 59, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '89b59224f9ad2c479618e983d55c11aa', 'text': "Although 5G NSA provides a good step from 4G in your journey toward 5G, it's not a full-fledged 5G SA deployment. There are also multiple variants of 5G NSA, and the choice of your deployment will depend on multiple areas such as your existing network topology, the existing bandwidth between the eNB and enhanced LTE eNB (ng-eNB), and your investment appetite.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 60, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a591c699e159407b0061c44dd08bcd72', 'text': 'This chapter takes you through the different options of 5G NSA and SA, including the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 60, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ccde0baaea4c6fbf75f02d45e8aeaae0', 'text': '• Evolution options from 5G NSA toward 5G SA as well as 4G and 5G interworking', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 60, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '75ca8b4f1d709b1fbfd49fa06cd086b2', 'text': '• Different options of non-public networks (NPNs) and public network integrated non-public networks (PNI-NPNs)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 60, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '17c2eaf7b180bbe8f99e207551368fab', 'text': '• New 5G LAN type deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 60, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9e685896e665269366931969a555861e', 'text': '• Deployments enabling network slice as a service (NSaaS) offerings', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 60, 'parent\_id': 'e6715184a541eb2a95d23f12501bc856', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1238bd0d6c9e7729438e8921dab60969', 'text': '5G NSA and SA Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 60, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b8c10976e30affa1d21ff1576701fbba', 'text': 'Two solutions are defined by 3GPP for 5G networks:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 60, 'parent\_id': '1238bd0d6c9e7729438e8921dab60969', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f99a6f2ae0b10f872535e13bd67136ae', 'text': '• 5G Non-Standalone (NSA): The existing LTE radio access and core network (Evolved Packet Core, or EPC) is used as an anchor for mobility management and coverage to add the 5G carrier. This solution enables operators to provide 5G services within a shorter timeframe and for less cost.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 60, 'parent\_id': '1238bd0d6c9e7729438e8921dab60969', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '476b64ed3c32d996c6911daa6c35dc21', 'text': '• 5G Standalone (SA): An all new 5G Packet Core will be introduced with several new capabilities built in. The SA architecture is composed of 5G New Radio (5G NR) and 5G Core Network (5GC). Network slicing, CUPS, virtualization, multi-Gbps support, ultra-low latency, and other aspects will be natively built in to the 5G SA Packet Core architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 60, 'parent\_id': '1238bd0d6c9e7729438e8921dab60969', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2e30a55b815dbd9d307f0cef9f39c88', 'text': 'Figure 2-1 illustrates the NSA and SA deployment options', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 60, 'parent\_id': '1238bd0d6c9e7729438e8921dab60969', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a4109ea053f7265635379076324b82fd', 'text': 'EPC 5GC Option 1: SA - LTE with EPC Option 2: SA - NR with 5GC Option 5: SA - LTE with 5GC EPC 56C 56C SA ((A)) ((A)) ((A)) NR LTE eNB Option 7:NSA - LTE & NR Option 3: - LTE & NR Option 4: NSA - LTE & NR with 5GC with EPC with 5GC 56C 56C EPC NSA ; e " asassa ((A)) \_((A)) ( A)) - ( A)) ( A)) o ( A)) LTE NR LTE NR LTE NR Ilear Dlana', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 61, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '61b06ce1d8f4a07cdd654fa10ea9f460', 'text': 'EPC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 61, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'PageNumber', 'element\_id': 'aea2611cf27590ac104da5e23fb686d9', 'text': '5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 61, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '372b079bc0819e69a6a460e55b33fc9f', 'text': 'Figure 2-1 NSA and SA Deployment Options', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 61, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '49b6ff02b5758f4be4fa2b01430ff322', 'text': '5G Non-Standalone (NSA) Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 61, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3276df8cda76480f29e465cbc355b222', 'text': 'The 5G Non-Standalone (NSA) solution enables operators using 4G EPC Packet Core to launch 5G services within a shorter timeframe and leverage the existing infrastructure. NSA leverages the existing LTE radio access and core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 61, 'parent\_id': '49b6ff02b5758f4be4fa2b01430ff322', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ce7a128b79986c4100035b3d0c086757', 'text': 'network (EPC) to anchor 5G NR using the dual connectivity feature. This solution provides a seamless option to deploy 5G services with very little disruption in the network. As shown in Figure 2-1, there are three primary options for NSA deployment: Option 3, Option 4, and Option 7. NSA Option 5 and 7 are based on using 5GC for supporting LTE deployments. NSA Option 3 is based on upgrading the existing LTE components, and the initial deployments of 5G are based primarily on this option.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 62, 'parent\_id': '49b6ff02b5758f4be4fa2b01430ff322', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b7e0f2a7a93e23b58e02c89dd12c4fa8', 'text': 'Option 3 has three variants, as described in the sections that follow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 62, 'parent\_id': '49b6ff02b5758f4be4fa2b01430ff322', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd8c67f1e3631886fdaab1979bb57d544', 'text': 'Option 3', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 62, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4bed15c4da83dce9b73a181c2b3eb490', 'text': 'In NSA Option 3, traffic is split across 4G and 5G at eNodeB, as illustrated in Figure 2-2.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 62, 'parent\_id': 'd8c67f1e3631886fdaab1979bb57d544', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '475df8eebd0161b7776b8e99120241d3', 'text': 'NSA Option 3', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 62, 'parent\_id': 'd8c67f1e3631886fdaab1979bb57d544', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ff2503ad61c68d0dd1d7ea2f9e185e00', 'text': 'NSA Option 3 Control Plane & User plane EPC Control Plane & User plane between the eNB & EPC \\ . between the eNB & gNB | S1-C§ S1-U Bt (p)-p - ((A)) LTE X2-U NR gNB) (eNB) i User Plane B S e S Control Plane UE', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 62, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5b50ad4b779b3fdd87a87075c5c3f955', 'text': 'Figure 2-2 5G NSA Option 3', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 62, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '763afb77306a05666bc95df7fbaed51c', 'text': 'The X2 interface is the interface between eNBs used in 4G and 5G NSA deployments; it performs the following control plane and user plane functions:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5294d369ef6b73a57df083c8008a70dd', 'text': '• Context transfer from source eNB to target eNB/gNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd7aef9c2b4af1a0746ca70c9053629a3', 'text': '• Control of user plane transport bearers between source eNB and target eNB/gNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a4320feba727d582d6aecd3a56db85de', 'text': '• Handover cancellation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f48cc5293c7939badec8f4db49018c5e', 'text': '• UE context release in source eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f96e7381522ce4f36f68d9c37d6ac89', 'text': '• Load management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0e9c0892df239fc8a95d2b021f1a58c5', 'text': '• Inter-cell interference coordination', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cd4197aadbed7703119c217e6560e536', 'text': '• Uplink interference load management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '077d7b8b3ff4e967f997b6b45e91cd04', 'text': '• Downlink interference avoidance', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '83e83adeb8e487a508cf4b16c52ca888', 'text': '• General X2 management and error-handling functions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e9f6f33f846c91aef4473e9d2930f1ca', 'text': '• Application-level data exchange', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5d7b7584b32ab2c90e8ac97222066c08', 'text': 'As shown in Figure 2-2, in NSA Option 3 deployment mode, both the user plane (X2-U) and control plane (X2-C) are required to be implemented between the 4G eNB and 5G gNB. For this reason (as compared to the other Option 3 deployment variants), this deployment option has the highest X2 traffic, specifically due to the X2-U traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'da5ac28d5dd9dcbc25acf60c13788a9f', 'text': 'Option 3a', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bf6e8d98a8f944d7844e58c622dc08bc', 'text': 'In NSA Option 3a, the traffic is split across 4G and 5G at EPC, as illustrated in Figure 2-3.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 63, 'parent\_id': 'da5ac28d5dd9dcbc25acf60c13788a9f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '52299c81aef27cea91af9f36cc942292', 'text': 'NSA Option 3a', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 64, 'parent\_id': 'da5ac28d5dd9dcbc25acf60c13788a9f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '85d9ebc8a2a82e2f167c095621b6aec5', 'text': 'NSA Option 3a User plane between gNB and EP EPC Control Plane & User plane Only Control Plane between the eNB & EPC \\ between the eNB & gNB 81-Ci 1/ W XZC LTE NR (eNB) (gNB) User Plane Control Plane UE', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 64, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a94c1a8dce6ba69553998d4b6297be3f', 'text': 'Figure 2-3 5G NSA Option 3a', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 64, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c9897ef5a6d75c57cb7a7f85681ca19f', 'text': 'As shown in Figure 2-3, in NSA Option 3a deployment mode, only the control plane is implemented between the 4G eNB and 5G gNB, and the user plane is implemented between the 5G gNB and the 4G EPC. As only the X2 control plane is implemented between the eNB and gNB, the traffic is quite sparse as compared to the 5G NSA Option 3 deployment mode.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 64, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8163a1635bb9144bf42a0818bc0de14f', 'text': 'Option 3x', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 64, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cde112b56353fb9e5205ab56fe6b95a9', 'text': 'In NSA Option 3x, the traffic is split across 4G and 5G at 5G gNB, as illustrated in Figure 2-4.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 64, 'parent\_id': '8163a1635bb9144bf42a0818bc0de14f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '83a6a15b659ef8ff22f552dd0f8ddef8', 'text': 'NSA Option 3x', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 65, 'parent\_id': '8163a1635bb9144bf42a0818bc0de14f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5172ba0249b0ff49c07928a01abbc8a4', 'text': 'User plane between gNB and EPC User plane EPC S1- U & EPC \\ | /. Control Plane & User plane between the eNB & gNB S1-C i S1 U 1 (VRER: .((A>) LTE X2-U NR (eNB) 9NB) i User Plane Control Plane UE', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 65, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '000eb794e943f1d94ae717aa20da9975', 'text': 'Control Plane & User plane between the eNB & EPC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 65, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'badb47a4edecfeb91aa535662c1ff1ab', 'text': 'Figure 2-4 5G NSA Option 3x', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 65, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2068bffcab9d8f6a485e39f0a679c5c4', 'text': 'As shown in Figure 2-4, in NSA Option 3x deployment mode, although the control plane and user plane are implemented between the 4G eNB and 5G gNB, the amount of user plane and control plane LTE traffic in these interfaces is quite negligible. The user plane is also implemented between the 5G gNB and the 4G EPC, which enables data to route directly to the NR gNB, thereby avoiding excessive user plane load (which was the case in Option 3) on the existing LTE eNB, which was designed for 4G LTE traffic load and not additional NR traffic load.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 65, 'parent\_id': 'badb47a4edecfeb91aa535662c1ff1ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '99c7da95f2270a012cf4131a760adf33', 'text': 'Among the three variants of 5G NSA Option 3, Option 3x is the widely deployed option. In this variant, the control plane is implemented in the 4G eNB, where the call can be anchored, thus providing good service continuity. Option 3x also has negligible impact on the transport catering for the X2 and', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 65, 'parent\_id': 'badb47a4edecfeb91aa535662c1ff1ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67c850afa48830b60bcca4b95c375d1e', 'text': 'S1 interfaces, which is one of the most expensive parts of the infrastructure and requires careful planning and configuration.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 66, 'parent\_id': 'badb47a4edecfeb91aa535662c1ff1ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '28845e3dea8c65adf109a0ccde409ae6', 'text': '5G Standalone (SA) Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 66, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c854eb20fcc722e9cbf1f161ba204884', 'text': 'For use cases such as enhanced mobile broadband (eMBB), the target key performance indicators (KPIs) are 4ms one-way latency, 10–20Gbps peak data rate, and 50–100Mbps user-experience data rate, which can be achieved by 5G SA Option 2 deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 66, 'parent\_id': '28845e3dea8c65adf109a0ccde409ae6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '46168c3c7aa0bfe389fc0909b376fbaf', 'text': 'Figure 2-5 illustrates one of the methods for evolving from 4G to 5G NSA and from 5G NSA to 5G SA.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 66, 'parent\_id': '28845e3dea8c65adf109a0ccde409ae6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd2684e7a487ebbd2ef602a3c7fbe0a88', 'text': 'Option 1: SA - LTE with EPC Option 3: NSA - LTE & NR Option 2: SA - NR with 5GC with EPC 5GC EPC EPC N2 N3 §1 S1U $1C 1 |S1-U St i - ((A)) ((A)) ( A)) - ( A)) eNB \\B eNB g\\NB User Plane T Control Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 66, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2d55f4d6d08bfcffeb1ff7f9d0a5b921', 'text': 'Figure 2-5 Standalone (SA) Options', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 66, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '76378254643b09923121bb7a2e21fca6', 'text': 'As shown in Figure 2-5, the existing service providers can choose to migrate to 5G NSA mode of deployment using Option 3, which is the most common step used by service providers. In 5G SA Option 2, the New Radio (NR) access network consisting of gNBs is connected to 5G Core (5GC). The user plane (UP) and control plane of SA Option 2 use NR and are completely independent', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 66, 'parent\_id': '2d55f4d6d08bfcffeb1ff7f9d0a5b921', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2fa3e01c357536244abc3eb594fe58c8', 'text': 'of Long-Term Evolution (LTE), and many deployments plan to cater for the distributed UP and CP implementations using multi-access edge compute (MEC).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 67, 'parent\_id': '2d55f4d6d08bfcffeb1ff7f9d0a5b921', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '07e12f4fa81851a84462aa70c499375c', 'text': '5G SA Option 2 has many deployment options based on the use case, industry vertical, and service offering planned by the service providers. In many cases, related to industry verticals such as smart manufacturing that require ultra- reliable low-latency communications (URLLC), high bandwidth, and integration with third-party applications, the edge computing platform and applications will be co-located with the User Plane Function (UPF). In cases where latency is not the primary requirement, only the automation part will need co-location with the UPF in the MEC. In cases where MEC is deployed on the gNB location, it will usually have limited hardware resources and site conditions and therefore require virtualization infrastructure with a very low footprint (for example, the size of the room), cooling, limited power supply, and so on. This can be achieved by ensuring that only critical services with container-based technology are deployed in the edge.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 67, 'parent\_id': '2d55f4d6d08bfcffeb1ff7f9d0a5b921', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '50eeb1602ece8145513e89ab72168688', 'text': 'With the 5G technology being used in diverse verticals, the requirements of building an open ecosystem and having interaction protocol refinement across multiple parties (including vendors and operators) are critical. This inherently necessitates flexibility in deployment of 5G-related network functions and applications. Integration with the public cloud and deployments of network functions on the public cloud are very much dependent on the regulations being stipulated per country, as some countries (specifically in Europe) have very strict regulations on public cloud deployment. Figure 2-6 illustrates the main locations where 5G network functions (NFs) could be deployed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 67, 'parent\_id': '2d55f4d6d08bfcffeb1ff7f9d0a5b921', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd52dae613bc93b4af8590ad38da2b828', 'text': 'On-premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 68, 'parent\_id': '2d55f4d6d08bfcffeb1ff7f9d0a5b921', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1d7d36876c8629e71089ede475de88ab', 'text': 'Multi-stack Public Cloud', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 68, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7865ce04186e776a22f54a3ef2a94bfc', 'text': 'Hybrid Cloud', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 68, 'parent\_id': '1d7d36876c8629e71089ede475de88ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '7e33b2769c978854f15964afee2187a0', 'text': 'il', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 68, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '271e90f0ab8d582bfca88f5219e6e822', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 68, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ce3aa1dd94e6d84d977734ff596bfd6c', 'text': 'E O', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 68, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '619f9228d480fa33a91a47217842287a', 'text': '5G CNFs deployed only on private cloud, programmable routers, low footprint servers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 68, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b70344f868249617de103d3ebbb0ffdf', 'text': '5G CNFs deployed only on public cloud providers (GCP, AWS, Azure and so on) & public cloud provided by 5G equipment vendors', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 68, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '49bee7bed6ae3b2b6111410739618612', 'text': '5G CNFs deployed on mix of on-premises & mult stack Public Cloud', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 68, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '19f0f7b3bf2955dc1cdd59a10ff07b20', 'text': 'Figure 2-6 Deployment Location Options for 5G Network Functions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 68, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '24f1c1de23235500e9aa514ef3a81c8f', 'text': 'Direct and Indirect Communication for NF and NF Service', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 68, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7774ef7866136559352bb559d15817aa', 'text': 'You can deploy 5G SA Option 2 in direct and indirect inter-NF communication models, as illustrated in Figure 2-7.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 68, 'parent\_id': '24f1c1de23235500e9aa514ef3a81c8f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '7709ea48070c00478290b48d6dafdba8', 'text': 'API API SCP Direct Communication Indirect Communication', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 69, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8356457fca295a6ad742bd67a699d24b', 'text': '5G NF: 5G Network Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 69, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ef1539b413778276940bdb6ce0feaa95', 'text': 'API: Application Programming Interface', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 69, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f18c33f54db58df3492127065726cb8', 'text': 'SCP: Service Communication Proxy', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 69, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '24e706c6f7dc0b535a91a800cf004a0c', 'text': 'Figure 2-7 Direct and Indirect Communication for NF and NF Services', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 69, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '59946948a91e0d75e6b07849176af425', 'text': 'The direct and indirect communication models for NF and NF services as specified in 3GPP Rel-16 are further explained next.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 69, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1bc092e64e45f54230dc532612925836', 'text': 'The direct model consists of two options:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 69, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '97bb5cdfb0c19e51f404e68e4efdb793', 'text': '• Model A: Direct communication without Network Resource Function (NRF) interaction. In this model, the NFs do not interact with NRF and there is no service discovery.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 69, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a21afb779ffc5f34340dc9b85b31ea9', 'text': '• Model B: Direct communication with Network Resource Function (NRF) interaction. In this model, the NFs interact with NRF for service discovery.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 69, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bf8339326e6b3b5d42024f26bd0700cc', 'text': 'The indirect communication model consists of the following two options:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 69, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '17458cf9a00caf7f4fc70bbce81e1b8b', 'text': '• Model C: Indirect communication without delegated discovery. In this model, Service Communication Proxy (SCP) is introduced in the NF communication path, which aggregates Hypertext Transfer Protocol (HTTP) links and provides monitoring of centralized signaling.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 69, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cd781ff269e369b46e6a6742f427de1d', 'text': '• Model D: Indirect communication with delegated discovery. In this model, SCP takes over service discovery and selection for NF consumers; hence, NF consumers no longer need to perform discovery and select service providers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 70, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '520f5b33715033dd85613f6e1d0bd8d9', 'text': 'You can deploy both the direct and indirect communication models at the same time in your network, depending on your architecture and the use case you are trying to achieve. The indirect communication model makes use of the Service Communication Proxy (SCP) network function, as shown in Figure 2-7. SCP was introduced in 3GPP Rel-16 and defined in 3GPP TS 23.501. Figure 2-8 illustrates the key functions of SCP, which are further explained in the list that follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 70, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'e46f856d91ea8852de7d2fb2fa4a2703', 'text': 'NRF \_@\_.II SCP2 ﬂ@ SCP ) TLS TLS SCP3 B e NF C1 0 (o ) NF C2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 71, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6364130fbb5794dd06f9a063a7980e53', 'text': 'Figure 2-8 Key Functions of SCP', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 71, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '805367eaaa2fdc787de41f7ebda0a1f2', 'text': '1. Centralized monitoring: SCP provides centralized monitoring, which is very critical to identify threats in 5G multivendor deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 71, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '30b3710b9e7f46bd1a9c6d0ff186c5c8', 'text': '2. Distributed SCP deployments: SCP can be deployed in distributed mode, enabling you to design the network in a flexible manner. SCP also provides message forwarding and routing to other SCPs in your network. In order to', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 71, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cb542a25fdd933e4fb65e5ec17ab9484', 'text': 'enable an SCP to route messages through several SCPs, an SCP can register its profile in the NRF. If NRF integration is not preferred, then a local configuration can be used to determine the SCP in the next hop.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 72, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6bea0d0f0342a890ed9dad1740171a0f', 'text': '3. Load balancing: SCP provides real-time congestion control, handling of overload conditions and message forwarding and routing between NF/NF service.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 72, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '03c727360e4a1a1872fa26ac07c9ce7a', 'text': '4. Resilient integration with third-party vendors and application developers: SCP provides communication authorization and continuous service discovery and selection for the NF consumers by selecting a different instance of NF. This ensures continuous service to the NF consumer and third-party vendors and application developers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 72, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c1368389e887e27adcb853487be6818f', 'text': '5. Encrypted communications: Apart from preventing unauthorized communications, SCP can also implement cryptographic verification using techniques such as Transport Layer Security (TLS)/mutual Transport Layer Security (mTLS). You can maintain complete control over the distribution of keys and certificates, with the vendors, application developers, and NF consumers completely detached from the process.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 72, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c18c39f3a153baab468af581fc5ebe95', 'text': 'The aforementioned features and functionalities of SCP provide added security to your 5G deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 72, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '644d1b986a5f80cb492049dfefc24458', 'text': '4G and 5G Interworking', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 72, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bef2159cc88327b0347ae0292b833ca2', 'text': '4G and 5G interworking must have inter–radio access technology (inter-RAT) handovers (HOs). Inter-RAT HO is supported by functions such as combined 4G and 5G subscription data access function (HSS and UDM), 4G and 5G control plane (PGW-C and SMF), and 4G and 5G user plane (PGW-U and UPF), as shown in Figure 2-9.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 72, 'parent\_id': '644d1b986a5f80cb492049dfefc24458', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '2bb9d418e8a165c98fae4d9fac9a53d2', 'text': 'Sba N8 HSS + UDM N10 PCF N15 N7 86-C PGW-C + SMF N11 N4 §5-U PGW-U + UPF SGW §1-U N26 AMF N2 §1-C N1 N3 i\\ ((A)) 4GeNB 56 gNB E-UTRAN) (NG-RAN)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 73, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f1398166ddd80397c40a5fa3002ef081', 'text': 'HSS - Home Subscriber Server', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 73, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2946862adad1ed4d2e2854ebcd20e93', 'text': 'UDM : Unified Data Management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 73, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'a50b396318eaf78496984b96664108cf', 'text': ': Policy Control Function PGW-C : PDN Gateway - Control Plane : Packet Data Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 73, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'e5b3da409b04107558b491b8017bdf87', 'text': 'PCF.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 73, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'aadba3d8822156cac2e5137fe94409d7', 'text': 'PDN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 73, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '53a3cd303f100033366681127eed4eaf', 'text': 'Figure 2-9 4G and 5G Interworking', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 73, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bf3c98b0908d32ace1e9f5e50d7a8a32', 'text': 'SMF : Session Management Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 73, 'parent\_id': '53a3cd303f100033366681127eed4eaf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1b8c8c799d23878f8cfff323cd8535bf', 'text': 'PGW-U: PDN Gateway - User Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 73, 'parent\_id': '53a3cd303f100033366681127eed4eaf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '65789081f2092a1406d38f2a3e210d54', 'text': 'UPF - User Plane Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 73, 'parent\_id': '53a3cd303f100033366681127eed4eaf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4a66d59f12496ea77027bc9bfc5ecfa6', 'text': 'SGW : Serving Gateway', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 73, 'parent\_id': '53a3cd303f100033366681127eed4eaf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9c27b4b5103305ee691d46274a23ad1f', 'text': 'MME Management Entity', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 73, 'parent\_id': '53a3cd303f100033366681127eed4eaf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4edb4bca70775bcd58d9661d770f176c', 'text': 'AN e AL M -', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 73, 'parent\_id': '53a3cd303f100033366681127eed4eaf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6637f7bce551125233243959bf3ad351', 'text': 'As shown in Figure 2-9, the 4G and 5G Radio Access Networks (RANs) have their own control plane and user plane implementations and work independently of each other, unlike 5G NSA, where there are some dependencies between 4G and 5G, depending on the Option 3 variants.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 74, 'parent\_id': '53a3cd303f100033366681127eed4eaf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67755781342a311a26a4183ba50da00f', 'text': 'The interworking is achieved by having combined 4G and 5G network functions in the packet core. The interworking includes idle mode and active mode procedures. Idle mode is when your phone is not on a call and is on a RRC\_IDLE state. Cell selection and reselection modes are used for moving between cells. In an active mode, the RRC state is RRC\_CONNECTED, and the same mechanism of moving between cells is called a handover.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 74, 'parent\_id': '53a3cd303f100033366681127eed4eaf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'befe60e7333575984a38a33e0b07f8a2', 'text': 'VRAN/O-RAN/C-RAN and Related Deployment Models', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 74, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '70252c19969179c626b81d0ce862c6f1', 'text': 'Virtualized RAN (VRAN) and Open RAN (O-RAN) are terms used in conjunction with each other, and though they are closely inter-linked, there are some differences between them.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 74, 'parent\_id': 'befe60e7333575984a38a33e0b07f8a2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '21d98c18066ad34cb895fd9ce76a4bee', 'text': 'VRAN relates to providing you with virtualized 4G and 5G network functions that can be deployed in any commercial off-the shelf (COTS) hardware server or multistack public cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 74, 'parent\_id': 'befe60e7333575984a38a33e0b07f8a2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d19a12a7f8926710265f5f807bbeed6', 'text': 'O-RAN, which is specified by the O-RAN Alliance, provides you with the ability to utilize machine learning systems and artificial intelligence backend modules to empower network intelligence through open and standardized interfaces in a multivendor network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 74, 'parent\_id': 'befe60e7333575984a38a33e0b07f8a2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '40118d099ad9754ed1bbf5fc9d567ee7', 'text': 'C-RAN has been known as Centralized, Clean, Cloud, and Collaborative RAN but is widely just called Centralized RAN or Cloud RAN. C-RAN uses open platforms and real-time virtualization technology rooted in cloud computing to achieve dynamic shared resource allocation of Centralized Unit (CU) and Distributed Unit (DU).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 74, 'parent\_id': 'befe60e7333575984a38a33e0b07f8a2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b9be55b577dd9817f53363f500a904de', 'text': 'This section will discuss O-RAN architecture and deployment options and then delve into C-RAN.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 74, 'parent\_id': 'befe60e7333575984a38a33e0b07f8a2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4f6104de29d06aa213bb2b9353fbc58b', 'text': 'Open RAN (O-RAN) deployments are driven by the requirements of open interface, flexible deployments and total cost of ownership (TCO) reduction. Figure 2-10 illustrates the O-RAN high-level architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 74, 'parent\_id': 'befe60e7333575984a38a33e0b07f8a2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c2342c967e978c02890583cc082c598d', 'text': 'pemmsssssssanan: P, O-RAN Architecture - Key Components External System Service Management and Orchestration (SMO) Framework E for Data Non-RTRIC enrichment O-RAN defined interface 02 Al 0 FH M-Plane LA e L L L LT LT T Ty B e A itk taietataiaiail Near-RTRIC NG — NG-Core i \\ O-RAN Network Functions (NFs) 3GPP defined interfaces O-RU =) L e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 75, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5dadb8da86bcd2140f20950e4b2b160c', 'text': 'Figure 2-10 4G and 5G High-Level O-RAN Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 75, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b8f20b1fbb24000af8012427b945c805', 'text': 'The key components of the O-RAN architecture are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 75, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f751d8c57bf50dafff6dc9ab02d5e239', 'text': '• Service Management and Orchestration framework: The Service Management and Orchestration (SMO) framework provides an integration fabric that enables orchestration and management of multivendor O-RAN Network Functions. The SMO framework also contains the Non-Real Time (Non-RT) RAN Intelligence Controller (RIC) function, which has the goal of supporting intelligent RAN optimization in non-real time (that is, greater than one second) by providing policy-based guidance using data analytics and AI/ML training/inference.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 75, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0acac9bff86ed395c1ffe698fa30e7dc', 'text': '• Non-RT RIC: The Non-RT RIC is a central component of the SMO, which enables non-real-time control and optimization of RAN elements and resources and support for AI/ML workflows. The Non-RT RIC provides fine-grained policy-based guidance to the Near-RT RIC through', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 75, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f92782727abce9aad08857f5bfa2b9c9', 'text': 'the AI interface and is composed of the Non-RT RIC framework and Non- RT RIC applications (rApps)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 76, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'def0aa782f2869c7ce800683b7194150', 'text': '• O-RAN Network Functions: The Network Functions for the radio access side consist of Near-Real-Time RAN Intelligence Controller (Near-RT RIC), Open-RAN Compatible Centralized Unit Control Plane (O-CU-CP), Open-RAN Compatible Centralized Unit User Plane (O-CU-UP), Open- RAN Compatible Distributed Unit (O-DU), and Open-RAN Compatible Radio Unit (O-RU). Figure 2-11 illustrates the planes of the O-RAN front- haul interface and its protocol stack.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 76, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '607f13c92d74cce5fa75c136baad9620', 'text': 'C/U - Plane O-RU S-Plane — 0-DU M-Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 76, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '52017ea7997a783747eda34333b7e88a', 'text': 'M-Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 76, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4e90d2bd6a2dc9124f3dca91ab20732b', 'text': 'CIU - Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 76, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '2a201b16751e3926ca34dc5ed0ee829d', 'text': 'eCPRI/RoE UDP (optional) IP (optional) Etheret L2 + VLAN Ethernet L1 e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 76, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5aec1de6117cb64d9933106a6275dc97', 'text': 'S-Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 76, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'afc5f20a447a1c8170a06092d823b0fd', 'text': 'PTP SyncE H Ethernet L2 Ethernet L1', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 76, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '1d2e05440ab7ed2ca731308417cb7a7d', 'text': '| s O', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 76, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'text': 'Figure 2-11 Details of Each of the Planes of the O-RAN Front-haul Interface', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 76, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dada13b2fcdb13daf380b709d8674362', 'text': 'The key functionalities of the C/U, S, and U planes are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 76, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '68e519e6b4ef87372a4d33355ad16eed', 'text': '• Control plane (C-Plane) messages provide:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 76, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd3164a9d83df39dc08d816ac37bc6488', 'text': '• Scheduling and beam-forming commands', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '65e3b8c80c2af75ec00f14fa0c1ed460', 'text': '• Downlink (DL) precoding configuration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '91ee2fddecefe3110baa0c44743db362', 'text': '• Physical random access channel (PRACH) handling', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c0072d4c4f782ccf1b9829a483b644cf', 'text': '• User plane (U-Plane) messages provide:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5dbdfabdac4faf0a71d0319c6b941b37', 'text': '• Support for data compression', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c3e01ff48ea45d20b4b52747b3f96543', 'text': '• In-phase and Quadrature Phase (I/Q) data transfer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cb124049f90a8fb12f2e0480f29a8c53', 'text': '• DL data precoding', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '84d240e95a9e2a561db45e6b9b04f0b5', 'text': '• Sync plane (S-Plane) provides:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3808b06a0649cfa22291eee49c0669bf', 'text': '• Timing and synchronization between O-RU and O-DU', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ec78f053dfdef03b482298daca65783c', 'text': '• PTP and SyncE profiles', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b6a0321fa93baceff5875c5f84e10354', 'text': '• Synchronization topologies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0a19f66d8130395dc1e2eeaf5f2fe652', 'text': '• Management plane (M-Plane) provides:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '27425cc0ffe709e1442d43360e235285', 'text': '• Support for hierarchical/hybrid model', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7bb520accd52ea925561ee5d97b8c31a', 'text': '• C/U plane IP and delay management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6403da9de6bcb3b7aa03833d5ebdd849', 'text': '• Fault, configuration, accounting, performance, security (FCAPS), including sync configuration and status', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e760bb6e106b3f610e7a8c79228510b2', 'text': 'SMO also utilizes the O1 interface for OAM toward the O-RAN Network Functions, except for the O-RU. For hybrid management, the Open FH M- plane is utilized between the SMO and the O-RU, while for hierarchical management the SMO manages the O-RU indirectly via the O-DU.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed7d4b1c8e4e3bd23678b8354c8fcc70', 'text': '• Near-RT RIC: Near-RT RIC enables near real-time control and optimization of O-RAN (O-CU and O-DU) nodes and resources over the E2 interface with near-real-time control loops (that is, 10ms to 1s). The Near-RT RIC uses monitor, suspend/stop, override, and/or control primitives to control the behaviors of O-RAN nodes. The Near-RT RIC hosts xApps that use the E2 interface to collect near-real-time RAN information to provide value-added services using these primitives, guided by the policies and the enrichment data provided by the A1 interface from the Non-RT RIC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '948608bec447f9b87da37d63c3e922b6', 'text': '• O-Cloud: O-Cloud facilitates flexible deployment options and service provisioning models of O-RAN virtualized network elements in telco', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 77, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7d068e047069f02cecd4fd4857702f4b', 'text': 'clouds. The O-Cloud is an infrastructure element (or collection elements) that is based on COTS servers, uses hardware accelerator add-ons as needed, and has a software stack that is decoupled from the hardware. O- Cloud will host the relevant O-RAN functions, the supporting software components, and the appropriate management and orchestration functions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 78, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ac8d6d20bf3a139abffab9e3c3c29964', 'text': 'There are multiple modes of O-RAN deployment, as shown in Figure 2-12. In the initial stage, CU/DU co-located deployment is more suitable, which can reduce E2E latency, CAPEX, time to market, and complexity in network planning and operation. Many implementations are also aimed at CU/DU split deployment, where the DU is located closer to the gNB. The CU is deployed at the edge site farther to the DU and aggregates multiple DUs. Due the flexibility of 5G NF deployments, the DUs, CUs, UPFs, and all other virtualized components of 5G can be deployed on multistack public cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 78, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '889202f6527d2ee75c01b6de81974993', 'text': 'Figure 2-12 illustrates the different deployment methods for O-RAN.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 78, 'parent\_id': '162aa6a7c0355d8cb00506f0a0a9ce58', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '8e5e2e339bc19d3333f0ed5ef674ee15', 'text': "((A)) —— FH BH 0-RU i4—> EOD | SO E E P — ((A)) MH BH FH E 0-RU \\i ' 0 :; ' 04U W— = = - R — ((A)) WH BH BH UPF 0-CU ESe— \\i i{ L — 00,000 g\\ /E i{ g ~OR. 56C FH: Fronthaul ((A)) UPF: User Plane Function BH CP: Control Plang MH: Midhaul 0-RU, 00U, 0-CU BH: Backhaul — MEC: Mult-Access Edge Compute RU: Radio Unit 5GC : 5G Packet Core DU: Distributed Unit CU: Centralized Unit \\ premmenssannnnnn——— E Private Cloud / On-premise DC P: User Plane (o oaup BH CP: Control Plang ((A) FH | UpF L 0-CU-UP Q Public Cloud E E App: Application 0-RU —! nm e", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 79, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2c7147b355e9e461a24436e95b5af5d0', 'text': 'Figure 2-12 O-RAN Deployment Options', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 79, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2dcdff9fd8e14931290819b2a44b1004', 'text': 'O-RAN Alliance and O-RAN-related communities are building partnerships and ecosystems to allow wider use of O-RAN. An example is the O-RAN Software Community (OSC), which is a collaboration between the O-RAN Alliance and Linux Foundation with the mission to support the creation of software for the RAN and Open RAN MoU Group of the Telecom Infra Project', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 79, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0993947d28d3dec649f63d644c664521', 'text': '(TIP), which supports the advancement and adoption of standards-based Open RAN solutions. Furthermore, O-RAN Alliance Security Focus Group (SFG) is mitigating security risks to reduce the likelihood and impact of attacks on third- party RAN applications, open front-haul interface, network management, and UE identify privacy within the O-RAN.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4fd00cdb6411fd801fb6b4b815ff02a1', 'text': 'Cloud RAN (C-RAN), which is also sometimes referred to as Centralized RAN, has the base band unit (BBU) deployed at the centralized location, which enables you with a lightweight deployment of Radio Unit (RU), which is also sometimes referred to as Radio Resource Unit (RRU) and Antenna at the cell site. In 5G, the BBU is further split into Distributed Unit (DU) and Centralized Unit (CU). C-RAN architectures use a front-haul interface between the BBU in the centralized core and the RU in the cell site, as shown in Figure 2-13. Although C-RAN provides several advantages, such as better resource virtualization, joint processing, and the possibility of cooperative radio sharing, it has yet to take off as a mainstream deployment option. As compared to C- RAN, O-RAN is seeing wider adoption due to the openness, cost effectiveness, and flexibility in deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'e9c361891d7634436a0554629088a3b7', 'text': '- - ((A)) T ————— BH UPF & 5GC CP emmmmmmmma——. FH RU U, CU components | Y ——— ‘i i{ lE =] \\i i{ -~ = - BBU (DU, CU) Pooling 5G C-RAN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '040f872639f20c0942610e9abaf5cf84', 'text': 'UPF: User Plane Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fc82d81835e812553857cc512eed3829', 'text': 'CP: Control Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cf77f9330c906326c06396e1d18ea431', 'text': 'BBU: Baseband Unit', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '95e200d03e6afb5cec850f0d63ad57af', 'text': '5GC : 5G Packet Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '573745d4a7d69ee179b445fb38ea4a3f', 'text': 'ﬁ', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '759faf17b0c484d0256063e983438ace', 'text': 'Private Cloud / On-premise DC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5901fd11e6e625d541337001093e29e3', 'text': 'Q', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5f0fcdc825049949804db32ce54ff300', 'text': 'Public Cloud', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a6ddff0c4ab0f3cd7044fc07983335c', 'text': 'FH: Fronthaul', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bb774d68a5cdf0d494dec430d54242d1', 'text': 'BH: Backhaul', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '151419de2673855d8d3560adf6380fa8', 'text': 'RU: Radio Unit', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '93a61f3db50a959487d0b43c5926471d', 'text': 'DU: Distributed Unit', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c3c6d4945a95fa83232983318267c71b', 'text': 'CU: Centralized Unit', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b4c93a8a1b79ec1cc599f00574a19458', 'text': 'C-RAN: Centralized RAN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 80, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Header', 'element\_id': '6fd80480817cdad71e486f8140334f50', 'text': 'Figure 2-13 C-RAN Deployment Example', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 81, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6af948604984a8bb049c89816c971c83', 'text': 'Network Slice as a Service (NSaaS)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 81, 'parent\_id': '6fd80480817cdad71e486f8140334f50', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a228c54090d357e8472b9edc9c39b239', 'text': '5G SA Option 2 also enables smart manufacturing/industry 4.0 by providing lower latency for URLLC by using edge computing and flexible deployment methods such as deploying 5GC Network Functions (NFs) in public cloud. These offerings can be made as a service by the service providers, as shown in Figure 2-9, using network slice as a service (NSaaS), thereby providing them with a new potential revenue source.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 81, 'parent\_id': '6af948604984a8bb049c89816c971c83', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4cc6a46458ea1ca099f1541c78f8e406', 'text': 'NSaaS can be offered by a communication service provider (CSP) to its customer service consumer (CSC) as a service. Note that some vendors refer to CSP as network slice provider (NSP) and CSC as network slice consumer (NSC).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 81, 'parent\_id': '6af948604984a8bb049c89816c971c83', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3fb43a423a50d89fd533fab11e9f3e88', 'text': 'Business-to-Everything (B2X)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 81, 'parent\_id': '6fd80480817cdad71e486f8140334f50', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '027bed64db2e6c3ef1fe2bea44876c3a', 'text': 'The network slice offered as a service to the CSC can be utilized to fulfil its requirements. This model is generally referred to the B2X model, which consists of business-to-business (B2B) and business-to-consumer (B2C) models and is illustrated in Figure 2-14. B2B is generally used for providing services from service providers/CSPs to enterprise or industry vertical customers, and B2C is aimed at providing Internet-related services to mass consumers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 81, 'parent\_id': '3fb43a423a50d89fd533fab11e9f3e88', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5b0195eb40c64d54404ce79e6a764fc7', 'text': 'Figure 2-14 shows the NSaaS deployment method for the B2X offering.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 81, 'parent\_id': '3fb43a423a50d89fd533fab11e9f3e88', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f8a5728a08b7c41918a0166a9f0e536f', 'text': 'e e ey \\ { S — R e = = <. 5 ettt it = APls Communication Service Provider Industry Verticals / Enterprises (CSP) / Network Slice Provider é : S Consumers N (NSP) S—— SS— | Communication Service Consumer I i (C AN - R e J————— 5GC CP and UP Transportlayer | PF,MEC A (<A>) E e gNB Tog Ill T R RRRE—— PR UPF: User Plane Function O Public Cloud CP: Control Plang o= Private Cloud / UP: User Plane &= On-premise OC MEC: Multi-Access Edge Compute 5GC : 5G Packet Core App: Application', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 82, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b898dc62a3c7dcfc72d8961eaeb7c2e7', 'text': 'O', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 82, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7711e7da674b323ea8c174a8e0fa3c01', 'text': 'Public Cloud', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 82, 'parent\_id': 'b898dc62a3c7dcfc72d8961eaeb7c2e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd9549569aac3e2e67ebf1b93be1ab9eb', 'text': 'Private Cloud /', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 82, 'parent\_id': 'b898dc62a3c7dcfc72d8961eaeb7c2e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8de35cfbe57f554e356f16be98d4ef4f', 'text': 'o=', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 82, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'a90e3542f6632a54164348c8cb105d5e', 'text': '&=', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 82, 'parent\_id': '8de35cfbe57f554e356f16be98d4ef4f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8aa33be7d789893e13134476634b7146', 'text': 'UP: User Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 82, 'parent\_id': '8de35cfbe57f554e356f16be98d4ef4f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1812a8e830261a23b08995a1d7e65249', 'text': 'On-premise OC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 82, 'parent\_id': '8de35cfbe57f554e356f16be98d4ef4f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '698fef4fe049ac3a4c311d2a1be7f91d', 'text': 'MEC: Multi-Access Edge Compute', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 82, 'parent\_id': '8de35cfbe57f554e356f16be98d4ef4f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed376db0249c799de568c80996a4c2f4', 'text': '5GC : 5G Packet Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 82, 'parent\_id': '8de35cfbe57f554e356f16be98d4ef4f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ff66c4047aab95572600e57a3ba88f2', 'text': 'Figure 2-14 NSaaS Deployment Method for B2X Offering', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 82, 'parent\_id': '8de35cfbe57f554e356f16be98d4ef4f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b19d2cb5cdac6432397c8dc8d1f668e9', 'text': 'Business-to-Business-to-Everything (B2B2X)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 82, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ec63aee30d0bb90383c6f49ebc60716f', 'text': 'The network slice obtained by the CSC can also be utilized to play the role of CSP and offer its own services on top the slice services offered by the primary CSP. These types of services, illustrated in Figure 2-15, are called B2B2X services.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 82, 'parent\_id': 'b19d2cb5cdac6432397c8dc8d1f668e9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'af27682d67203148dbfb9b01ddf4a58d', 'text': "S CSP/NSP D R i i iSBii I APls Service Layer Communication Service Provider CSP) / Network Slice Provider : | T —— | E NSP) I — S—— E Industry Verticals / Enterprises 1 Congumers 5GC CP and UP é scvsscessessssanassasetsesssassreneres é Transportlayer UPF, MEC App Communication Service Consumer i ((A)) é } Oﬂ é (CSC)/ Network Slioe Consumer (NSC) ,' i v AT i g\\B 0\_ - UPF: User Plane Function 0 Public Cloud CP: Control Plane UP: User Plane = Private Cloud &= Onpremise OC MEC: Mult-Access Edge Compute App: Application 5GC : 5 Packet Core", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '26dbc260d021fcb7d779925979f17191', 'text': '0', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1bfd39e6e5411816f0e02c79b8e42cb5', 'text': 'Public Cloud', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7d0f29d78203d7e19503fe209d12b6d2', 'text': 'UPF: User Plane Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e28afa0bdb082680a4d2cc650cb6eac7', 'text': 'CP: Control Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f4cb9d52b06d4f4672d0853fb4c5d251', 'text': 'Private Cloud', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '03ab07700586b1073bc6195eae347351', 'text': '= &=', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd1896817d51373d388ad3c1623756849', 'text': 'UP: User Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2daf0492fc301e27667e949ed7f808cd', 'text': 'Onpremise OC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '25e67166307658196c72d803d344f3a6', 'text': 'MEC: Mult-Access Edge Compute', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aaf27537906b943a7b75144a051b2a46', 'text': '5GC : 5 Packet Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8fb76237b94a440e4699f2d051b5afe0', 'text': 'App: Application', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b29af97a820cfb245e8a39811666e409', 'text': 'Figure 2-15 NSaaS Deployment Method for B2B2X Offering', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c4a38d7b5b93ede56fbcd7a9a4d6247c', 'text': 'Depending on the service offering, the CSP offering NSaaS can impose certain limits on the NSaaS management capabilities exposure to the CSC, and the CSC can manage the network slice according to NSaaS management capabilities exposed and agreed upon in the SLAs between the CSP and CSC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'parent\_id': 'b29af97a820cfb245e8a39811666e409', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b0d41dfdc072a2d886e816ec1affe6fa', 'text': "The NSaaS offered by the CSP could be characterized by certain KPIs and SLAs. Here's a list of some sample KPIs:", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'parent\_id': 'b29af97a820cfb245e8a39811666e409', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '65727442156f2f15eadaf7a80c2a9a93', 'text': '• Type of Radio Access Technology (RAT)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'parent\_id': 'b29af97a820cfb245e8a39811666e409', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '52c684a9ac4afb5a640ee89b3d5e7000', 'text': '• Minimum Guaranteed Downlink (DL) Throughput', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'parent\_id': 'b29af97a820cfb245e8a39811666e409', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4c037a6dbafe97511aa8099a58f31dda', 'text': '• Minimum Guaranteed Downlink (UL) Throughput', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 83, 'parent\_id': 'b29af97a820cfb245e8a39811666e409', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8f1367a4890e8a52b49c7c7b2dc479a6', 'text': '• Maximum Latency', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 84, 'parent\_id': 'b29af97a820cfb245e8a39811666e409', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '617f24b6f40979790cecac2b8ae7a628', 'text': '• Minimum Availability', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 84, 'parent\_id': 'b29af97a820cfb245e8a39811666e409', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1472725c1347ca785976a559ef16102a', 'text': '5G Time-Sensitive Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 84, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aae9eac9a619bc4d1b4fd281bddb84c1', 'text': 'The key advantages of deploying 5G technology are realized when 5G can be integrated and converged with existing and upcoming technologies being used in industry verticals and enterprises to enable new use cases such as smart industry 4.0, smart factory, and so on. For this to happen, 5G systems should work hand in hand and be integrated with the IEEE 802.1 working group covering time-sensitive networks (TSNs).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 84, 'parent\_id': '1472725c1347ca785976a559ef16102a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c9cf885bb8ef7bcbde87c5e25897113d', 'text': 'The IEEE TSN set of specifications is aimed at convergence and enabling low- latency communication in the factories of the future. 5G Time-Sensitive Communication is a service that supports deterministic and/or isochronous communication with high reliability and availability. It provides packet transport with quality of service (QoS) characteristics such as bounded latency and reliability, where end systems and relay/transmit nodes can be strictly synchronized.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 84, 'parent\_id': '1472725c1347ca785976a559ef16102a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '210ebafd85bbb170cc297031d381924d', 'text': 'When 5G is used to support TSN, the whole 5G system (5GS) is considered to be a TSN bridge. For 5GS to act as a TSN bridge, it needs to be time aware. This requires 5GS to be compliant with IEEE 802.1AS, which is an adaptation of Precision Time Protocol (PTP) for use with time-sensitive networks. To achieve this, TSN translators (TTs) are deployed at both the edge of the network—at the UE side and the UPF side—as shown in the Figure 2-16. The TT at the UE side is called the device-side TSN translator (DS-TT) and the TT at the UPF end is called network TSN translator (NW-TT). When 5GS needs to support a TSN flow, a PDU session will be initiated with QoS characteristics, as required by the TSN traffic flow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 84, 'parent\_id': '1472725c1347ca785976a559ef16102a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '2304903fc85a9d20bccda060b5cf19bf', 'text': 'PECT L e 5G System SBA based 5GC / ( A)) 4—> oNB [Ty P —) TSN End Device ~ TSN Flow TSN End Device', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 85, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6a5ecd84efd1538939e1c0c43845eba8', 'text': '5G PDU Session - Delay Critical GBR QoS Flow', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 85, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '3e12ee8278fc09691819ad7ea1385849', 'text': 'UPF: User Plane Function NW-TT: Network Side TSN Translator 5GC. 5G Core SBA: Service Based Architecture TSN: Time Sensitive Nefwork UE: User Equipment DS-TT: Device Side TSN Translator (GBR: Guaranteed Bit Rate PDU: Protocol Data Unit', 'metadata': {'text\_as\_html': '<table><tbody><tr><td>UPF: User Plane Function</td><td>NW-TT: Network Side TSN Translat</td></tr><tr><td>SBA: Service Based Architecture</td><td>5GC. 5G Core</td></tr><tr><td>TSN: Time Sensitive Nefwork</td><td>UE: User Equipment</td></tr><tr><td rowspan="2">DS-TT: Device Side TSN Translator</td><td>(GBR: Guaranteed Bit Rate</td></tr><tr><td>PDU: Protocol Data Unit</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 85, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b7e6c4c158fe51ad0521ee13d9c3a3d', 'text': 'UE: User Equipment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 85, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '23f0da659bad91103b0cf29d3abe6af5', 'text': 'PDU: Protocol Data Unit', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 85, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8166152fbbea28383715406631d1aeb6', 'text': 'Figure 2-16 TSN Flow in 5G System', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 85, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '12a5a931b1f4bb741e0fdd749262d05e', 'text': 'To maintain timing synchronization, UE, gNB, UPF, and TT will use the 5GS grandmaster (GM) clock to maintain synchronization. For the TSN domain synchronization, the GM in the TSN domain will be used. The PDU sessions with the specific QoS flows will be established based on the Application', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 85, 'parent\_id': '8166152fbbea28383715406631d1aeb6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d831380ad78260d8620a253fa47e54c', 'text': 'Function (AF) TSN translator integration with 5GC via the Network Exposure Function (NEF) or Policy Control Function (PCF), as shown in Figure 2-17. The AF TT is also integrated with the central network controller (CNC), which defines the schedule for transmitting TSN frames. To maintain time synchronization between the TSN and 5GS domain, the following procedure is followed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 86, 'parent\_id': '8166152fbbea28383715406631d1aeb6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5369798cbd4977a17f5ea84c7ace43ac', 'text': 'Whenever the UPF receives the PTP message from the TSN domain, it will be sent to the DS-TT via the UE using the PDU session. The DS-TT will include the time taken for the packet to traverse from NW-TT to DS-TT in the egress PTP message before it sends it to the TSN domain. This time taken for the packet to traverse from the NW-TT to DS-TT is called the calculated reference time. By adding the calculated reference time to the egress PTP message, the accuracy of the PTP timing information is maintained.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 86, 'parent\_id': '8166152fbbea28383715406631d1aeb6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ae48f1de91df91bf008d5d8923c61980', 'text': 'ammmm————— cmmmmeny 5GS acting as TON Bridge / 5GS GM UDM NEF f AMF SMF PCF CNC (y) mssssssssssssssnannnnnn e— “ l\\ gum-- L e T\\ TSNGM TSN Flow TSN GM', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 87, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'f40df26b0fdd48ae0d8bebe2a4ddd362', 'text': 'UPF: User Plane Function NW-TT: Network Side TSN Translator SBA: Service Based Architecture 5GC: 5G Core TSN: Time Sensitive Network UE: User Equipment DS-TT: Device Side TSN Translator GM: Grandmaster clock AF TT: Application Function TSN Translator SMF: Session Management Function NEF: Network Exposure Function UDM: Unfied Data Management PCF: Policy Conirol Function CNC: Central Network Controller', 'metadata': {'text\_as\_html': '<table><tbody><tr><td>UPF: User Plane Function</td><td>NW-TT: Network Side TSN Translator</td></tr><tr><td>SBA: Service Based Architecture</td><td>5GC: 5G Core</td></tr><tr><td>TSN: Time Sensitive Network</td><td>UE: User Equipment</td></tr><tr><td>DS-TT: Device Side TSN Translator</td><td>GM: Grandmaster clock</td></tr><tr><td>AF TT: Application Function TSN Translator</td><td>SMF: Session Management Function</td></tr><tr><td>NEF: Network Exposure Function</td><td>UOM: Unified Data Management</td></tr><tr><td>PCF: Policy Conirol Function</td><td>CNC: Central Network Controller</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 87, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '39a63f2c21fc903a88fc9d98b9431f14', 'text': 'UE: User Equipment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 87, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fe172f384d8ee8e0ebe538dd1fea4eb2', 'text': 'SMF: Session Management Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 87, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '33d1d1dc8e011762f823cc6643274550', 'text': 'UDM: Unfied Data Management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 87, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '06367a4c3c968e51634f9772100bdf7a', 'text': 'CNC: Central Network Controller', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 87, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3bf5cfafbc9a269394df727d5ae0cb64', 'text': 'Figure 2-17 Maintaining Timing Synchronization Between 5GS and TSN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 87, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ccb0e0e8f86b0493e1d57ca92de0a69', 'text': 'Domains', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 87, 'parent\_id': '3bf5cfafbc9a269394df727d5ae0cb64', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cb42410bd9370d6826e91c2441009597', 'text': "Ongoing work to enhance TSN support for 5G-related use cases is prolific. The IEC/IEEE 60802 joint project is currently defining a TSN profile specification for the TSN features to be supported for industrial automation. This will enable interoperability, testing, and certifications. The Open Platform Communications (OPC) Foundation's Field Level Communications (FLC)", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 87, 'parent\_id': '3bf5cfafbc9a269394df727d5ae0cb64', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'efd623e02b484da08355a8d42d9df2fc', 'text': 'initiative also aims to provide specifications based on IEC/ IEEE 60802 to achieve a single common multivendor converged TSN network infrastructure. 3GPP Release 17 (Rel-17) will bring in further enhancements to provide enablers for time-sensitive communications and time synchronization.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 88, 'parent\_id': '3bf5cfafbc9a269394df727d5ae0cb64', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '93d91c94a8489e675cf3204e5e933d92', 'text': '5G Local Area Network–Type Service', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 88, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0818f60cfac2a55a95240ddd3278062c', 'text': 'The real value of 5G is realized when we extend the scope of 3GPP-defined technologies to industry verticals and enterprises. Looking at the enterprise deployment scenarios, there are use cases such as local area networks (LANs) that can be fulfilled by 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 88, 'parent\_id': '93d91c94a8489e675cf3204e5e933d92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '93decf69199cb7a1ad6484f62498f3d8', 'text': '5G LAN-type services are being introduced by 3GPP, which provides LAN- type abstraction to 5G user equipment (UE) to send packets across the 5G network. The functionalities provided by 5G LAN-type service will be similar to your LAN, including support of virtual networks (VNs), which are termed 5G LAN–virtual networks (5G LAN-VNs). For example, in the enterprise environment, the UE in the 5G VN group can communicate with each other within a 5G VN. The Network Exposure Function (NEF) also exposes services to dynamically manage the 5G VN group data. Furthermore, 5GS supports optimized routing by enabling support for local switching at the UPF without having to traverse the data network for UE-UE communication when the two UE(s) are served by the same user plane function.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 88, 'parent\_id': '93d91c94a8489e675cf3204e5e933d92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6d75d4ff2edbe0f1ff9ae64980039706', 'text': 'Three types of traffic-forwarding methods are allowed for 5G VN communication, as listed next:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 88, 'parent\_id': '93d91c94a8489e675cf3204e5e933d92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cd91cdd59bfbb5c922e091e9f31040c4', 'text': '• N6-based: In this method, the UL/DL traffic for the 5G VN communication is forwarded to/from the DN; Figure 2-18 illustrates the non-roaming user plane architecture to support 5G LAN-type service using N6 tunnel.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 88, 'parent\_id': '93d91c94a8489e675cf3204e5e933d92', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'fd0c17606eeec4d03fc91b405d128f05', 'text': 'UE 1 N3 UPF N6 (R) AN DN UE 2 UPF (R)AN N3 N6', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 89, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1101e069e627d46dcb1f27422ab59c16', 'text': 'UE: User Equipment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 89, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5926ba0a99b505974791b56f5de44f63', 'text': 'UE: User Equipment (R)AN: Radio Access Node or Access Node UPF: User Plane Function DN: Data Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 89, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '19f3b2b44c7b9485753ea37662a622da', 'text': '(R)AN: Radio Access Node or Access Node', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 89, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9aece28381c3e008002a0d23d533da58', 'text': 'UPF: User Plane Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 89, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0ad8bc286b70014066702c2a86c48387', 'text': 'DN: Data Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 89, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '30cb0a93d549ff68921f759e16e0a75f', 'text': 'Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 89, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ecb7760bdd1b946c43873c41e5c6d02', 'text': 'Figure 2-18 N6-Based Traffic Forwarding for 5G LAN-Type Service Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 89, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed2bb6cb527f8c3cc457c115996acd05', 'text': '• Local switch based: In this method, the traffic is locally forwarded by a single UPF if this UPF is the common PSA UPF of different PDU sessions for the same 5G VN group. Figure 2-19 illustrates the non- roaming user plane architecture to support 5G LAN-type service using a local switch.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 89, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5f5993402adc7d097826230f510088d8', 'text': '- - UE 1 N3 — -UPF N9 (R) AN PSA - - UPF - - (Local UE 2 (R)AN N§ — -UPF — Ng Switch) - -', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 90, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3bc66521265062641791fb8ae597e4c3', 'text': 'UE: User Equipment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 90, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '417687682fb7bddd4ee758c5e9473e06', 'text': 'UE: User Equipment (R)AN: Radio Access Node or Access Node [-UPF: Intermediate User Plane Function PSA: PDU Session Anchor', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 90, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c0f028e5d3970798e23a1ae7f11c622b', 'text': 'Figure 2-19 Local Switch–Based Traffic Forwarding for 5G LAN-Type Service Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 90, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dd3443e7ae604216e6ab77f5b826f7ef', 'text': 'Service Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 90, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '59379c1a91747b38a1613939f41f8b10', 'text': '• N19-based: In this method, the UL/DL traffic for the 5G VN group communication is forwarded between PSA UPFs of different PDU sessions via N19. N19 is based on a shared user plane tunnel connecting PSA UPFs of a single 5G VN group. Figure 2-20 illustrates the non- roaming user plane architecture to support 5G LAN-type service using N19 tunnel.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 90, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a5549782a68d4d9b84140ca82fdff36c', 'text': "UE1 N3 — IUPF' (R)AN oL l ( UE 2 (R)AN N3—' l-UPF ‘—N9 = 3", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 91, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fb6d5d2196f7f8d31c23eb0129a8d61c', 'text': 'UE: User Equipment (R)AN: Radio Access Node or Access Node [-UPF: Intermediate User Plane Function PSA: PDU Session Anchor', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 91, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'efbbb5dd2d92e9e8451d892150d23833', 'text': 'UE: User Equipment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 91, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6425e559fc2a4c0eefcea5ce0d46dc35', 'text': '(R)AN: Radio Access Node or Access Node', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 91, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a80dc394716366973e1eecc9971fa89d', 'text': 'PSA: PDU Session Anchor', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 91, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fe8b9a1f47d90144954f81fe9d185655', 'text': 'Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 91, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '334810e1c90da4ace112410b43142112', 'text': 'Figure 2-20 N-19-based Traffic Forwarding for 5G LAN-Type Service Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 91, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '875e5973c2dccac2786e0de5eccd1946', 'text': 'Depending on the policy defined by the service provider, the 5G network shall allow trusted third parties to perform dynamic management of 5G VN group identification and membership. The Network Exposure Function (NEF) exposes a set of services to manage (for example, add/delete/modify) the 5G VN group and 5G VN member.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 91, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '909c8457a6c8ef28a2267751c412a494', 'text': 'Private 5G/Non-Public Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 91, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '55d2129c6348cd5b27cbf4e9e2f06caf', 'text': '5G SA Option 2 will also serve vertical industry use cases. To address these use cases, the network exposure capability and network slicing feature are defined to ensure openness, SLAs, isolation, and ease of use. 5G deployments that are implemented specifically to fulfill the industry verticals or enterprise use cases are called non-public networks (NPNs). NPNs are also referred to as private 5G networks. NPNs are intended to be used by the private enterprises or industry verticals and are not for general public use.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 91, 'parent\_id': '909c8457a6c8ef28a2267751c412a494', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '747bc3caaf298fc01b2143e1e4115b84', 'text': 'The two types of NPN networks are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 91, 'parent\_id': '909c8457a6c8ef28a2267751c412a494', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3e93cd592f3de3417b8b81f532de48bf', 'text': '• Standalone non-public network (SNPN): SNPNs are usually operated by an industry vertical such as smart manufacturing factories or critical', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 91, 'parent\_id': '909c8457a6c8ef28a2267751c412a494', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e811f740f978ac19c5c1a7c3c8b342e5', 'text': 'infrastructure that want to operate their own 5G network and do not rely on traditional mobile network operators/service providers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 92, 'parent\_id': '909c8457a6c8ef28a2267751c412a494', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '88ae1bd3d59c271688b8c635057578a8', 'text': '• Public network integrated non-public network (PNI-NPN): PNI-NPNs rely on traditional mobile network operators/service providers—for example, an enterprise that obtains a slice using an NSaaS offering from the CSP/NSP.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 92, 'parent\_id': '909c8457a6c8ef28a2267751c412a494', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f19a0fff9231fd959639083dda2e8021', 'text': 'Standalone Non-Public Network (SNPN)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 92, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed5a4cdb271055b093ff5dc9dba4c078', 'text': 'The flexibility and openness offered by 5G allows industry verticals and large enterprises to deploy their own 5G network and become NPN operators. Radio spectrums—sets of frequency ranges for cellular-compatible mobile devices to connect to a cellular network—can be owned by the NPN operator or can be leased from service providers based on the country radio regulations and the chosen operating model.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 92, 'parent\_id': 'f19a0fff9231fd959639083dda2e8021', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '59e0aa7249ad4a02ec42e85e25141781', 'text': 'SNPN Radio Access Network (RAN) broadcasts public land mobile network identity (PLMN ID) and network identity (NID) in the system broadcast, enabling network (re)selection, overload control, access control, and barring. In addition, 3GPP Release-16 also specifies the capability for UE to obtain PLMN services while camping on the standalone non-public RAN. This enables the NPN operators to essentially “whitelist” the subscribers/users/endpoints they want on their network and manage them. The devices will be configured with a subscription permanent ID (SUPI) and will follow the usual registration procedures as being performed in the public networks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 92, 'parent\_id': 'f19a0fff9231fd959639083dda2e8021', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a996f0d77d86475a7c4c8205de75971c', 'text': 'Looking at various deployment models that could be implemented by NPN operators, it would be good to have a simplified comparison with the Wi-Fi deployments in the enterprise. As illustrated in Figure 2-21, a Wi-Fi deployment will consist of many Wi-Fi access points (AP), which are actually radio nodes using the 2.4 and 5 GHz radio spectrums in the Wi-Fi architecture, spread across your campus. These APs are then aggregated by the aggregation switches and forwarded to the wireless LAN controller (WLC). The WLC has integration with AAA servers, which perform authentication, authorization, and accounting for the users and devices. Roaming and handovers are also performed between the Wi-Fi APs based on the mobility of the users and devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 92, 'parent\_id': 'f19a0fff9231fd959639083dda2e8021', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '39ab223eb47905cebb0c1acb6814e851', 'text': 'In summary, the key components of Wi-Fi architecture in the example shown Figure 2-21 are the Wi-Fi APs and the WLC. Access and aggregation switches', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 92, 'parent\_id': 'f19a0fff9231fd959639083dda2e8021', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '09728d04bae08f424c1c8c58fc3df0d6', 'text': 'are of course important, but the primary components that are “pure” Wi-Fi are still the APs and WLCs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 93, 'parent\_id': 'f19a0fff9231fd959639083dda2e8021', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '9b29923caa5546dbe7305422d677269a', 'text': 'Enterprise / Industry Veertical Private Network (dentity and Access A Management & Global Policy Engine Primary WiFi components Authentication Authonzatlon and L) Accounting / ,..-..--..\\ [T Applications [ 3 -))) [T Infra @ g - &8 -u\_ ) i w (@ -\_\_ Public Cloud Users & WiFi Access 1 Access & Wireless LAN Devices \\ Points Aggregation P TS TR T Controller [TDC Applications and “esssseses switches Internet Enterprise IT & DC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 93, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3aada0f23f9ee420619e3baf72d2e5bb', 'text': 'Figure 2-21 Wi-Fi Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 93, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '285897bbe10c442dcd1f904521bfa995', 'text': "Now let's look at one of the methods of 5G NPN deployment where the end-to- end 5G component, including the radio spectrum, is catered by an enterprise or industry vertical. Here, along with the Wi-Fi radio node, commonly called a Wi-Fi access point (AP), you can also deploy the 5G radio node, called the gNB. 5G and Wi-Fi technology can co-exist with each other, as they use different radio spectrums, thereby preventing any interference between them.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 93, 'parent\_id': '3aada0f23f9ee420619e3baf72d2e5bb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8b05fc0f67ebf20e7298d886835b37dd', 'text': 'If you plan to go for the O-RAN/VRAN deployment model, you will use the disaggregated version of the gNB, which is the Distributed Unit (DU) and Centralized Unit (CU), along with the RAN intelligent controller (RIC). The gNBs are then aggregated using the access and aggregation switches and then terminated at the 5G Core (5GC), as illustrated in the Figure 2-22. The authentication, authorization, and accounting of the users and devices are enabled by integrating your existing authentication, authorization, and accounting (AAA) solution. The policy that is to be applied to the users and devices is configured within the Global Policy Engine in your existing Identity and Access Management (IAM) solution. There are also deployment models', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 93, 'parent\_id': '3aada0f23f9ee420619e3baf72d2e5bb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1e0c5761c26ab40978ae49b1d50ba7a2', 'text': 'for SNPN based on shared spectrum, and this would depend on the country regulations and business model of the NPN operator.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 94, 'parent\_id': '3aada0f23f9ee420619e3baf72d2e5bb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '14342b8d35c66797466cfb6cc78ad3cc', 'text': "Enterprise / Industry Vertical Private Network Identty and Access 1AM Management & Global Primary 5G components Policy Engine Authentication, Authorization and Accounting / N\\ PELLLLET susssssqessenan, [T Applications [ 3 E E i e B @ ((A)) 5GC (o) i w --E ' 56 Radio ‘ = = Public Cloud Users & | Node (gN) | Access & \\ Applications and Devices ITDC YT Aggregation Internet switches Enterprise [T & DC", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 94, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1499345699a08e0b9bf673bd34d63c2a', 'text': 'Figure 2-22 Non-Public Network Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 94, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0d47b61f19ab3b40d929bb0d43f06191', 'text': 'Figure 2-23 shows a detailed view of 5GC components for standalone 5GC deployments, with the 5GC network functions that are involved in the authentication process for standalone NPN deployments within enterprises or industry verticals.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 94, 'parent\_id': '1499345699a08e0b9bf673bd34d63c2a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c817044af9eeb2646beaa4a259aec434', 'text': 'Enterprise / Industry Vertical Private Network PIET TR, Identity and Access AM Management & Global Policy Engine Primary 5G components UDR Authentication, Authorization and PCF Accounting /\\ SMF Prerayay [T Applications [ 3 -)) E : ((A)) \\ ; U G i - - | """ (%] UPF - = ) 5G Radio l Users & Access & [ T ——— =g E Public Cloud Devices Node (gNB) | T0C Applications and Sesesees Aggregation Internet switches Enterprise IT & DC AMF - Access and Mobilty Management Function UPF - User Plane Function AUSF - Authentication Server Function Uom - Unffied Data Management SMF - Session Management Function UDR - Unified Data Repository PCF - Policy Control Function AAA Authentication, Authorization and Accouning 0e Data Center AM - Identity and Access Management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '265ffad723ee4ea4f56fb89318dff9f2', 'text': 'UPF - User Plane Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c36d1085ab62ec2182f98efba00d6cf8', 'text': 'AMF - Access and Mobilty Management Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7ca8c9cfcb11a8858d6f7a5a2453b031', 'text': 'Uom - Unffied Data Management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '171b1e3741352cb68cae3ae1478a6296', 'text': 'AUSF - Authentication Server Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2be9205cafbd742d8bbe9ed9c4af60b8', 'text': 'UDR - Unified Data Repository', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '28a2c0f31ed7af58d09fcd71424a5a3a', 'text': 'SMF - Session Management Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4d4b7a5caf21fba14bede393099470cc', 'text': 'PCF - Policy Control Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a6df76562ba5a976bed10d9b9d39c4a', 'text': 'AAA Authentication, Authorization and Accouning', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '763ff6c9b650ce6ece4904536b97cbdb', 'text': 'AM - Identity and Access Management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a17f1c575ee8a3ec66b961381f4f0e6f', 'text': '0e Data Center', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da07806a03737e0d1c2b1a540cae1c69', 'text': 'Figure 2-23 Non-Public Network Architecture—Detailed View', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '94485a97e26f23298422ca18892103ff', 'text': 'Public Network Integrated Non-Public Networks (PNI-NPN)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a2b7b68d28a83ac575a18c8e0b87e05', 'text': 'In public network integrated non-public network (PNI-NPN), network selection and reselection are based on PLMN ID. Cell selection and reselection as well as access control could be optionally based on Closed Access Group Identity (CAG ID). The CAG cell shall broadcast information such that only the UE supporting CAG is accessing the cell, which enables the PNI-NPN operator to control the users/devices that can access the network. When an', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 95, 'parent\_id': '94485a97e26f23298422ca18892103ff', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1600318c781ec000f81b6a2835e05b53', 'text': 'NSaaS offering is obtained by the NPN operator, the user devices can be preconfigured with Single Network Slice Selection Assistance Information (S- NSSAI) to allow access to specific slices serving the NPN.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 96, 'parent\_id': '94485a97e26f23298422ca18892103ff', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2cf96a7f18b1c21365cdb9a318b2fb61', 'text': 'PNI-NPN could be seen as an option, where some 5GC Network Functions (NFs) such as the User Plane Function (UPF) are deployed by the NPN operator and rely on the public network for other NFs. The primary methods of deployment for PNI-NPN are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 96, 'parent\_id': '94485a97e26f23298422ca18892103ff', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '40ab6fe08fc505058128c7f4ce241502', 'text': '• Hybrid Method A: NPN UPF integrated with control plane from SP', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 96, 'parent\_id': '94485a97e26f23298422ca18892103ff', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7c64a648042490386bb5a9d63d938e43', 'text': '• Hybrid Method B: Control plane shared with SP', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 96, 'parent\_id': '94485a97e26f23298422ca18892103ff', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'df413a8aea64bf4641fa036b1c9520fa', 'text': '• Network Slice method', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 96, 'parent\_id': '94485a97e26f23298422ca18892103ff', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'da8d4ff2c8339e2ee17af902b6f9edd1', 'text': 'Hybrid Method A: NPN UPF Integrated with Control Plane from SP', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 96, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d98da5a294fcac769cfb7bb17b36d90', 'text': 'Figure 2-24 illustrates one of the PNI-NPN deployment methods where the UPF and MEC applications are owned and deployed by you in your enterprise IT data center, public cloud, or in a hybrid manner, where the UPF is located in your private cloud/enterprise DC, and MEC applications along with the MEC platform manager and orchestration are deployed in the public cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 96, 'parent\_id': 'da8d4ff2c8339e2ee17af902b6f9edd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '13520dadcac038fdce28ad0ca0fac998', 'text': 'The radio spectrum used for capacity and coverage can be owned by you as an enterprise/industry vertical or could be shared spectrum with the service provider (SP) in your country, which is dependent on country regulations and the chosen business model.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 96, 'parent\_id': 'da8d4ff2c8339e2ee17af902b6f9edd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58d5fa05d852b810c9a90e7d0fe61487', 'text': 'This deployment method will allow you the flexibility to have complete control over the configuration of the radio access network (RAN) nodes, which are indicated in the Figure 2-24 as gNB, along with the User Plane Function (UPF) and MEC application deployments. The Control Plane Functions of the SP will need to be integrated with your gNB and UPF network functions. Depending on the use case, you will also need integration with the UPF of the SP. In such cases, the UPF deployed in the enterprise infrastructure will act as an Intermediate User Plane Function (I-UPF), which is essentially a relay function that directs the GPRS Tunnelling Protocol (GTP) with header extensions for 5G toward the UPF deployed in the SP MEC. The UPF deployed in the SP MEC will act as a UPF PDU session anchor, which terminates the GTP protocol. Depending on the use case (such as Identifier Locator Separation [ID-', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 96, 'parent\_id': 'da8d4ff2c8339e2ee17af902b6f9edd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c8760c7ad44c3dbc1183bf5e6be4758f', 'text': 'LOC] solution), Locator/ID Separation Data Plane (LISP-DP) protocol or identifier location addressing (ILA) could also be used to support migration into ID-LOC native network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 97, 'parent\_id': 'da8d4ff2c8339e2ee17af902b6f9edd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'b937c6a87552c66bcc171148e30ccb34', 'text': "UPF and MEC owned by Private 5G / NPN Network ) NPN operator / Entepise u\\N/Pubnc\\\\ cloud Private cloud Control Plane shared with SP UPF, MEC (Private) Radio Node | | Private or fomSPor | Shared o Spectum ith SP operator - ¢ — AMF, SMF, UDM, UPF, MEC (Publc) PCF, 56C CP ! ((A) ' = -0 gNB O O Internet/ MEC Centralized 56C Data Network : s A)) oNB Public Network", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 97, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e16ae20f3e074af869a67aa2c93786c', 'text': 'Figure 2-24 Hybrid Method A: NPN UPF Integrated with Control Plane from Service Provider', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 97, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4c16cd38e4d5fb7c1250bf324813eace', 'text': 'Hybrid Method B: Control Plane Shared with Service Provider', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 97, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f560eb0607b526cbbea59a7405a2dba7', 'text': 'Figure 2-25 illustrates one of the PNI-NPN deployment methods where the UPF, MEC applications, and parts of the 5G control plane are owned and deployed by you in your enterprise IT data center, public cloud, or in hybrid cloud. The control plane in this deployment method is shared with the service provider (SP). Depending on what 5G components are shared with the SP, it can be termed as RAN sharing, core sharing, or RAN and core sharing. In the example shown in Figure 2-25, the control plane part of the 5GC is shared with', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 97, 'parent\_id': '4c16cd38e4d5fb7c1250bf324813eace', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '060151b2c5d28b2aa7f120d304c91ea1', 'text': 'the SP and can be termed the core-sharing PNI-NPN deployment method if the RAN is managed by the NPN operator. If the RAN is also managed by the SP, it can be termed the RAN- and core-sharing PNI-NPN deployment method. The option for radio spectrum used for capacity and coverage is the same as the Hybrid Method A, which means that the radio spectrum can be owned by you as an enterprise/industry vertical or could be shared radio spectrum with the service provider (SP) in your country, which is dependent on country regulations and the chosen business model.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 98, 'parent\_id': '4c16cd38e4d5fb7c1250bf324813eace', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c6af6547e425c43f629c3c99df94f5a4', 'text': 'Private 5G / NPN Network Shared 5G Control Plane PERRE— Network Functions Entepise LAN/PubHc\\\\ cloud / Private cloud UPF, AMF, SMF, Radio Node NEF, MEC (Private) Private or from SP or Shared o Shecum operalor N with SP - ¢ m— UDM, PCF, UPF, MEC (Public) 5GC CP d (A) o P S e T = -0 : | —— NB O Internet/ MEC Centralized 5GC Data Network — =0y g\\B Public Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 98, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '679c0e9d67de8f46014d1f9090e47314', 'text': 'Public Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 98, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3911201cbab93e3238d3d8093aa52e8d', 'text': 'Figure 2-25 Hybrid Method B: Control Plane Shared with SP', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 98, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'be0c75164e1280af033eacc38ad0d095', 'text': 'Network Slice Method', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 98, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '14e87e05132e38a229fb3e7a1e936198', 'text': 'In PNI-NPN deployments using the network slice approach, the NPN network obtains the network slice from the service provider, which manages the control plane and user plane. Some deployments in the network slice method might only utilize the control plane method. This purely depends on the use case. Figure 2-26 illustrates the network slice PNI-NPN deployment method, where', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 98, 'parent\_id': 'be0c75164e1280af033eacc38ad0d095', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '69e18d22cf7f255f3cfb38f8e192a51d', 'text': 'an end-to-end network is deployed and managed by the SP. You as an enterprise or industry vertical might choose to deploy the UPF and MEC applications to cater for the URLLC use cases for Internet of Things (IoT) and industrial IoT (IIoT) deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 99, 'parent\_id': 'be0c75164e1280af033eacc38ad0d095', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '024a2a7fceba26d0103aa2bd55b2eaf3', 'text': '[Prvale%/NPN » FLKE SO b SR oy j —— ‘\\ Enterprise LAN/ Public cloud / Private cloud UPF, MEC Slice 1: Public Slice (Private) Local Break out -] Radio Node from SP Slice 1: SMF, PCF, UPF Slice 2: SMF, PCF, UPF el NFs common for all Slces: Spectrum Slice 1: UPF, MEC App A i Slice 2: UPF UDM, NSSF, AMF, NEF gNB ™ B8 —— —0) | IO— 5GC CP h« Internet/ Data Slice 2: Private / NPN Siice MEC O Network Centralized 5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 99, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'cbb6d88044b89401ab8610af6e3baa6b', 'text': 'Figure 2-26 Network Slice Method', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 99, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eb423ca8411ab255edfb169a129adfd3', 'text': 'As shown in Figure 2-26, Slice 1 caters for devices in the public slice and Slice 2 caters for the devices in the NPN network. You can choose to have the Local Break Out (LBO) deployed in your enterprise LAN by implementing MEC applications and user plane function for low-latency requirements of URLLC use cases. This method of deployment can be fulfilled by obtaining the NSaaS offering from the SP. You can agree to the SLAs and the KPIs with the SP to ensure the required QoS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 99, 'parent\_id': 'cbb6d88044b89401ab8610af6e3baa6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e6493c5c05c51fd4f1a1d0aacc328480', 'text': 'There are many more PNI-NPN deployment methods that vary in complexity and functionality based on the network function being deployed and the openness you plan to have on your deployment. Here are some of the key points you have to consider before choosing the deployment models:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 99, 'parent\_id': 'cbb6d88044b89401ab8610af6e3baa6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ce81149d6b7d16eb262c5e44f7720e21', 'text': '• The key use cases you plan to fulfil using 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 99, 'parent\_id': 'cbb6d88044b89401ab8610af6e3baa6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1afb3232949f3dc5252e856477ff26c1', 'text': '• The maturity level of expertise in your organization to manage 5G and evolving architectures.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 100, 'parent\_id': 'cbb6d88044b89401ab8610af6e3baa6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'af5363bedbabcc28e10e0f3f704df8b4', 'text': '• Analyze whether your use cases can be fulfilled by using a shared model with service providers for 5G RAN, transport, and core networks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 100, 'parent\_id': 'cbb6d88044b89401ab8610af6e3baa6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6b1c74a2045ff01eeeba89c3cab3b0d9', 'text': '• Choose whether you plan to own the radio spectrum yourself or share it with the SP.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 100, 'parent\_id': 'cbb6d88044b89401ab8610af6e3baa6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd32d0dfbe6121e9c83c1a2cdf168fbf9', 'text': '• Have a plan to train your key personnel regularly on cellular technologies (5G and beyond).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 100, 'parent\_id': 'cbb6d88044b89401ab8610af6e3baa6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '53ee7407de279d3b7fabd231290f590b', 'text': '• Decide whether you want a more open network deployment model such as O-RAN or want to use 3GPP-based distributed architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 100, 'parent\_id': 'cbb6d88044b89401ab8610af6e3baa6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8b5e06e2f07e6fb1bc4f30773a1ea63c', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 100, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '04b212ec5f6ef0c1974ccf64b753ad27', 'text': '5G Standalone (SA) is crucial not only for public network deployment but also for enabling industry verticals to deploy private 5G/non-public networks, thereby enhancing the existing industrial networks to smart industry 4.0, smart manufacturing, and addressing other key emerging use cases. 5G also allows you to monetize your network investments by allowing you to offer services to industry verticals using a NSaaS offering.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 100, 'parent\_id': '8b5e06e2f07e6fb1bc4f30773a1ea63c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '881b049f92fcf11403614062620197ce', 'text': '3GPP provides multiple architectures and deployment models for 5G, allowing service providers and industry verticals to choose the best-suited deployment model. Some choose the option of transitioning from 4G to 5G NSA and then from 5G NSA to SA, thereby taking a step-by-step approach. Some choose to deploy 5G SA directly without transitioning from 4G to 5G NSA.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 100, 'parent\_id': '8b5e06e2f07e6fb1bc4f30773a1ea63c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '18ba7bf993be75e19ed5ce7af318e720', 'text': 'There are other deployment models where you have the option of implementing 5G NSA or SA network functions on virtualized infrastructure within your premises, such as in your data centers, on a lightweight x86 server in remote sites, on programmable cell site routers, on a hybrid on-premises and public cloud, or entirely on a public cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 100, 'parent\_id': '8b5e06e2f07e6fb1bc4f30773a1ea63c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9d02e7fd343df69145c7742f5e670321', 'text': 'You can further make full use of the openness and flexibility in 5G architecture by opting to deploy O-RAN models and optimize your investments by choosing the best-of-the-breed vendors for specific parts of your 5G network buildout.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 100, 'parent\_id': '8b5e06e2f07e6fb1bc4f30773a1ea63c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4f7127bc8e675c785ad54b580d9473db', 'text': 'Before you choose any deployment model, it is best to understand the use cases you are trying to achieve, your target customer or industry vertical, and the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 100, 'parent\_id': '8b5e06e2f07e6fb1bc4f30773a1ea63c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '206cb9b71e644754733814a89e0a2576', 'text': 'strengths of your existing team. For example, if you are primarily a cloud service provider, then it might make more sense to build 5G network functions in your cloud infrastructure and then offer your 5G services to your customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 101, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '733bf82a59cbc7377a7ba35cf223cfc0', 'text': 'Acronym Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 101, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '556296ba9880771e4de1a56df42118e9', 'text': 'Acronym Expansion 5G LAN-VN 5G local area network—virtual network 5GC 5G Core network AF-TT Application function TSN translator AP Access point API Application programming interface BH Back haul CU Centralized Unit DL Downlink DS-TT Device-side TSN translator DU Distributed Unit eMBB Enhanced mobile broadband eNB E-UTRAN NodeB EPC Evolved Packet Core FH Front haul New Radio NodeB gNB', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Acronym</th><th>Expansion</th></tr></thead><tbody><tr><td>5G LAN-VN</td><td>5G local area network—virtual network</td></tr><tr><td>5GC</td><td>5G Core network</td></tr><tr><td>AF-TT</td><td>Application function TSN translator</td></tr><tr><td>AP</td><td>Access point</td></tr><tr><td>API</td><td>Application programming interface</td></tr><tr><td>BH</td><td>Back haul</td></tr><tr><td>CU</td><td>Centralized Unit</td></tr><tr><td>DL</td><td>Downlink</td></tr><tr><td>DS-TT</td><td>Device-side TSN translator</td></tr><tr><td>DU</td><td>Distributed Unit</td></tr><tr><td>eMBB</td><td>Enhanced mobile broadband</td></tr><tr><td>eNB</td><td>E-UTRAN NodeB</td></tr><tr><td>EPC</td><td>Evolved Packet Core</td></tr><tr><td>FH</td><td>Front haul</td></tr><tr><td>gNB</td><td>New Radio NodeB</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 101, 'parent\_id': '733bf82a59cbc7377a7ba35cf223cfc0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '99bcd7074b6020ce05f5b9e47b945694', 'text': 'HW Hardware M2M Machine-to-machine MBB Mobile broadband MEC Multiple-access edge compute MH Mid haul NPN Non-public network NR New Radio NSaaS Network slice as a service NW-TT Network-side TSN translator 0-CU O-RAN-compliant Centralized Unit O-DU O-RAN-compliant Distributed Unit O-RAN Open RAN O-RU O-RAN-compliant Radio Unit PDU Protocol Data Unit PLMN Public land mobile network PNI-NPN Public network integrated NPN SNPN Standalone non-public network TLS Transport Layer Security TSN Time-sensitive network TT TSN translator UE User equipment UL Uplink', 'metadata': {'text\_as\_html': '<table><thead><tr><th>HW</th><th>Hardware</th></tr></thead><tbody><tr><td>M2M</td><td>Machine-to-machine</td></tr><tr><td>MBB</td><td>Mobile broadband</td></tr><tr><td>MEC</td><td>Multiple-access edge compute</td></tr><tr><td>MH</td><td>Mid haul</td></tr><tr><td>NPN</td><td>Non-public network</td></tr><tr><td>NR</td><td>New Radio</td></tr><tr><td>NSaaS</td><td>Network slice as a service</td></tr><tr><td>NW-TT</td><td>Network-side TSN translator</td></tr><tr><td>0-CU</td><td>O-RAN-compliant Centralized Unit</td></tr><tr><td>O-DU</td><td>O-RAN-compliant Distributed Unit</td></tr><tr><td>O-RAN</td><td>Open RAN</td></tr><tr><td>O-RU</td><td>O-RAN-compliant Radio Unit</td></tr><tr><td>PDU</td><td>Protocol Data Unit</td></tr><tr><td>PLMN</td><td>Public land mobile network</td></tr><tr><td>PNI-NPN</td><td>Public network integrated NPN</td></tr><tr><td>SNPN</td><td>Standalone non-public network</td></tr><tr><td>TLS</td><td>Transport Layer Security</td></tr><tr><td>TSN</td><td>Time-sensitive network</td></tr><tr><td>TT</td><td>TSN translator</td></tr><tr><td>UE</td><td>User equipment</td></tr><tr><td>UL</td><td>Uplink</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 102, 'parent\_id': '733bf82a59cbc7377a7ba35cf223cfc0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'b97eea636eba0756c03eba7b194cff2a', 'text': 'UPF User Plane Function URLLC Ultra-reliable and low-latency communications WLC Wireless LAN controller X2-C X2—control plane X2-U X2-user plane Xn-C Xn—control plane Xn-U Xn—user plane XnAP Xn Application Protocol', 'metadata': {'text\_as\_html': '<table><thead><tr><th>UPF</th><th>User Plane Function</th></tr></thead><tbody><tr><td>URLLC</td><td>Ultra-reliable and low-latency communications</td></tr><tr><td>WLC</td><td>Wireless LAN controller</td></tr><tr><td>X2-C</td><td>X2—control plane</td></tr><tr><td>X2-U</td><td>X2-user plane</td></tr><tr><td>Xn-C</td><td>Xn—control plane</td></tr><tr><td>Xn-U</td><td>Xn—user plane</td></tr><tr><td>XnAP</td><td>Xn Application Protocol</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 103, 'parent\_id': '733bf82a59cbc7377a7ba35cf223cfc0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd2e6233480de4f059b99bfad3701d5df', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 103, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '73a10f7483b4335f45bc87c6b206fa33', 'text': 'Pramod Nair, “Securing Your 5G Infrastructure to the Edge and Beyond,” Cisco Public, April 1, 2021', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 103, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '864072b5fe91d1f69b3c251600f70e17', 'text': 'Pramod Nair, “Securing 5G and Evolving Architectures,” Cisco Knowledge Networks, Cisco Public, September 17, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 103, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3e56da29d650e9d48946e485364d6f49', 'text': 'Pramod Nair, “Why 5G is Changing Our Approach to Security,” Cisco Public, July 10, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 103, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a26f8850ec0ec6c328302479472847e2', 'text': 'Cisco Systems, “Reimagining End-to-End Network Mobile Network in the 5G era,” Cisco Public, 2019', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 103, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'be5e123f26a372bb59ad1dd88bec2ee4', 'text': '3GPP TS 24.301, “Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS): Stage 3”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 103, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aa122c8d49374adba90f99b66685d351', 'text': '3GPP TS 38.300, “NR: NR and NG-RAN Overall Description”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 103, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1428309257f3797aedd6ab79fad9c839', 'text': '3GPP TS 38.460, “NG-RAN: E1 general aspects and principles”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 103, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2c3f5d2123112ed788d3f08e83722f57', 'text': '3GPP TS 38.470, “NG-RAN: F1 general aspects and principles”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 103, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '37753c409e1722db35c9c8cc3e85803b', 'text': '3GPP TR. 23.374, “Study on Enhancement of 5G System (5GS) for Vertical and Local Area Network (LAN) Services”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 103, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '53464f7d543d876a075b0baf4da6bbb5', 'text': '3GPP TS 22.101, “3rd Generation Partnership Project: Technical Specification Group Services and Systems Aspects; Service aspects; Service principles”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 103, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8e4b56d934cd561bc54d1574e1532684', 'text': '3GPP TS 23.222, “Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 103, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b032fdfab7686459569a3b4672af551e', 'text': '3GPP TR 28.822, “ Study on charging aspect of 5G LAN-type Services” Rel-17', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 104, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e6d0fa50da531d7080892a03acd2785e', 'text': 'O-RAN Xhaul Packet Switched Architectures and Solutions 1.0, November, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 104, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '18128140091821bfb6d45d8316278987', 'text': '3GPP TS 32.290, “5G system: Services, operations and procedures of charging using Service-Based Interface (SBI)”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 104, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2bc3cd6aadf1d2f8d997efee3c0889a5', 'text': 'ETSI GS MEC 003, Multi-access Edge Computing (MEC); Framework and Reference Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 104, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9b859b6b9f605c351440655113363234', 'text': 'ETSI GS MEC 003, Multi-access Edge Computing (MEC);', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 104, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '890560d9f829bdb06ca1f754f089fcf2', 'text': 'Framework and Reference Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 104, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '44ffa5bc849d84b726d2f8c16ea3cc87', 'text': 'O-RAN Minimum Viable Plan and Acceleration towards Commercialization, White Paper - 29 June 2021', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 104, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9f5b461e971b517275df9edc95760980', 'text': 'https://5g-acia.org/whitepapers/integration-of-5g-with-time- sensitive-networking-for-industrial-communications/', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 104, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ea52c28282306c18e913a79e53a3d4ef', 'text': 'GSMA, “5G Implementation Guidelines: SA Option 2”. https://www.3gpp.org/', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 104, 'parent\_id': 'd2e6233480de4f059b99bfad3701d5df', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'text': 'Chapter 3. Securing 5G Infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd7dc8a0244573cbc5fc0552a54815a88', 'text': 'After reading this chapter, you should have a better understanding of the following topics:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c15b848349b1d6992793c80b542512f5', 'text': '• Security enhancements in 5G as compared to 4G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5ed31783a5c04c6050377a0d276cc484', 'text': '• Key 5G security enhancements in 3GPP Rel-16', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0fc49951de4a86db31c4de064fb91eb0', 'text': '• Key security challenges in 5G deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e3ff66a5126bf136bf03120ac748c7c6', 'text': '• Need for an external layer of security for 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ccc30fbc2a2987e2eccc1f518bc0cc24', 'text': 'As seen in previous chapters, not only will 5G technology usher in a new era of improved network performance and speed; it will also offer new connected experiences for users and fulfill various use cases for industry verticals. This chapter discusses the reasons why you should have an external layer of security controls even though 3GPP provides some enhancements in security.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '235e6df5c0a8f87b4bfb4a1ed7c668db', 'text': 'This chapter will be of particular interest to the following individuals and teams from enterprise/5G service providers deploying 5GC and cybersecurity vendors planning product developments for 5G security use cases:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '420fe4415f183257a452ec8c226a937c', 'text': '• Security leaders within government organizations who need to prioritize investments in security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '37882ffca9c559000b2a2b5d8a915ad6', 'text': '• Management consultants advising governments and service providers on 5G security investment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '10405d8831405341497162a8a1c400e6', 'text': '• CSO and CTO teams from service providers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'acdeb959fc255e15610c7d4e7c764d1a', 'text': '• CSO and CTO teams from enterprises deploying NPN/private 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b566d4b5afb1a8f36b10084400300e6c', 'text': '• CTO teams from service providers planning to offer network slice as a service (NSaaS)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2c7ea0efc1b9f39bb11b6930ee639290', 'text': '• Cybersecurity vendor security architects looking to secure 5GC deployments for their customers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c3ef49dc8edbd21aba75445b46a248ab', 'text': '• Cybersecurity vendor product managers looking for use cases or features to enhance security products to cater for secure 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '35252deba02f8f1c917c3a395ee78020', 'text': '• Teams and personnel from service providers, industry verticals, and military sectors who would like to get a brief understanding of security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 105, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8313cef75394470864a842d824224ef6', 'text': 'enhancements and security challenges in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 106, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '292ab8e867bc189c138787d488fb6bb4', 'text': '5G use cases will unlock countless applications, enable more robust automation, and increase workforce mobility. Incorporating 5G technology into these environments requires deeper integration between enterprise networks and the 5G network components of the service provider. This exposes enterprise owners (including operators of critical information infrastructure) and 5G service providers to risks that were not present in 4G. An attack that successfully disrupts the network or steals confidential data will have a much more profound impact than in previous generations.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 106, 'parent\_id': '50d834fa36e0237a3b7f8c7bb272c958', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9553c4a14eac9540e11c317b9c551555', 'text': '3GPP 5G Security Enhancements', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 106, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8c09915ce180ef1ea52482f8846127db', 'text': 'As compared to 4G, 5G brings in a unified, access-agnostic and flexible authentication framework that caters for 3GPP and non-3GPP users and devices, allowing different types of credentials. This has again been enhanced in 3GPP Release 16 (Rel-16), and further enhancements are being planned in Release 17 (Rel-17) to allow secure integration with non-public networks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 106, 'parent\_id': '9553c4a14eac9540e11c317b9c551555', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f21c7f1d3db7816078d67ffd2874ee5a', 'text': 'The 5G security architecture is designed to integrate 4G security. In addition, other security threats, such as attacks on radio interfaces, signaling plane, user plane, masquerading, privacy, replay, bidding down, man-in-the-middle, and inter-operator security issues, have also been taken into account for 5G. The enhancements to the security will be seen in upcoming releases, depending on the use cases and features being considered for the release, and this will be an on-going activity.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 106, 'parent\_id': '9553c4a14eac9540e11c317b9c551555', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4d9cf6e3386b1a48f05171fe1e42ebd6', 'text': '5G also improves subscriber identity protection by evolving the security for the initial Non-Access Stratum (NAS) messages. 5G also enables 5G Core (5GC) Network Function (NF) to be securely exposed via the Network Exposure Function (NEF). For the roaming interface, 5G introduces Security Edge Proxy Protection (SEPP), which protects the roaming interconnections between the home and visited networks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 106, 'parent\_id': '9553c4a14eac9540e11c317b9c551555', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9f2607dbc95182c1ee94bf4955685298', 'text': 'The sections that follow discuss some of the key security enhancements in 5G as compared to 4G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 106, 'parent\_id': '9553c4a14eac9540e11c317b9c551555', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '11dcf95064ee1c104d028bc21be31954', 'text': '5G Trust Model: Non-Roaming', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 106, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '564b7913a3542a7bc70442fae78fb787', 'text': '5G Standalone (SA) architecture evolves the trust model, where the trust within the network is considered as decreasing when moving away from the 5G packet core.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 107, 'parent\_id': '11dcf95064ee1c104d028bc21be31954', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b965065cd5199335a011ee40788957ba', 'text': 'Figure 3-1 illustrates the 5G trust model for non-roaming.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 107, 'parent\_id': '11dcf95064ee1c104d028bc21be31954', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '42fc141131548e97cf16ce8d06663ff8', 'text': 'Terminates Access Terminates Non- Holds the anchor Holds the key for - Does user Holds the re-use after Stratum Securty ~ Access Stratum ey /root key for identification, authentication A Security VPLMN authentication authentication credentials credential generation etc TN TR UD USIM ANF AUSF US AR g\\B UE 5G Control Plane Source: 3GPP Trust model of non-toaming scenario', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 107, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '61b5683078f2f7678757db816384df65', 'text': 'Source: 3GPP Trust model of non-toaming scenario', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 107, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'eed8d119ac5e9539b2aa253aedeb0c7d', 'text': 'Figure 3-1 Trust Model for 5G Non-Roaming Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 107, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0675b22c6dfa1775d3a368fbfbbcf87b', 'text': 'The trust model for the user equipment (UE), Radio Access Network (RAN) nodes, and 5G packet core is detailed in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 107, 'parent\_id': 'eed8d119ac5e9539b2aa253aedeb0c7d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3ddae063a012349eca4efe7c6a66c51c', 'text': '• UE: The tamper-proof universal integrated circuit card (UICC) on which the Universal Subscriber Identity Module (USIM) resides as a trust anchor, along with the mobile equipment (ME). The ME and the USIM together form the UE.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 108, 'parent\_id': 'eed8d119ac5e9539b2aa253aedeb0c7d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5d8c875e59e3944d4513ba3992d1b75a', 'text': '• RAN: The RAN is split into Distributed Unit (DU) and Centralized Unit (CU), as shown in Figure 3-1.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 108, 'parent\_id': 'eed8d119ac5e9539b2aa253aedeb0c7d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c3e76b206b680bcfb2b0844541dac32c', 'text': '• Distributed Unit (DU): The DU consists of DU-CP and DU-UP. The DU performs rate adaptation, channel coding, modulation, and scheduling as well as provides support for the lower layers of the protocol stack. It can be deployed together with the Radio Unit (RU)/Remote Radio Unit (RRU) or can be deployed in the far edge/edge layer where it serves multiple RUs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 108, 'parent\_id': 'eed8d119ac5e9539b2aa253aedeb0c7d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a7cd85cf2457781330390bdcfad5c0a9', 'text': '• Centralized Unit (CU): The CU consists of CU-CP and CU-UP. The CU caters for the Radio Resource Control (RRC) protocol, Service Delivery Adaptation Protocol (SDAP), and Packet Data Convergence Protocol (PDCP) as well as terminates the Access Stratum (AS) security. the CU can be co-located with the DU, or it can be deployed on far edge or edge layer and aggregates multiple DUs. The CU-UP and CU-CP split can also be performed to enable deployment of CU- UP closer to the DU.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 108, 'parent\_id': 'eed8d119ac5e9539b2aa253aedeb0c7d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3c4abf78168f64eace305cf390a02043', 'text': '• 5GC control plane:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 108, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e85ca8c0a96182a76c21640324af57f1', 'text': '• AMF: The Access Management Function (AMF) serves as the termination point for Non-Access Stratum (NAS) security.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 108, 'parent\_id': '3c4abf78168f64eace305cf390a02043', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a35f54cd74a156fbff73871744c736ff', 'text': '• SEAF: The Security Anchor Function (SEAF) supports the primary authentication using Subscription Concealed Identifier (SUCI) and holds the root key (known as anchor key) for the visited network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 108, 'parent\_id': '3c4abf78168f64eace305cf390a02043', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3784d1d0995d2566290b25f08cd6c349', 'text': '• AUSF: The Authentication Function (AUSF) keeps a key for reuse, derived after authentication, in case of simultaneous registration of the UE in different access network technologies (that is, 3GPP access networks and non-3GPP access networks such as IEEE 802.11 wireless local area network).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 108, 'parent\_id': '3c4abf78168f64eace305cf390a02043', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '31460f1b6da1ca02c85a65605b16133e', 'text': '• ARPF: The Authentication Credential Repository and Processing Function (ARPF) keeps the authentication credentials. This is mirrored by the user equipment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 108, 'parent\_id': '3c4abf78168f64eace305cf390a02043', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bad991a120e04666f400c89af086f40a', 'text': '• UDM: Unified Data Management (UDM) holds the home network private key for the private/public key pairs used for subscriber privacy.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 109, 'parent\_id': '3c4abf78168f64eace305cf390a02043', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f79a12680dac9989cd20798158a41acd', 'text': '5G Trust Model: Roaming', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 109, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '08ce69d33daee77b256bfbb170f641d9', 'text': 'In the roaming architecture, the home and the visited network are connected through Security Protection Proxy (SEPP) for the control plane of the internetwork interconnect. This enhancement is done in 5G because of the number of attacks coming to light recently, such as key theft and re-routing attacks in SS7 as well as network node impersonation and source address spoofing in signaling messages in DIAMETER that exploited the trusted nature of the internetwork interconnect.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 109, 'parent\_id': 'f79a12680dac9989cd20798158a41acd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '65afcbe20199c1c1a36b81f3328ef5e4', 'text': 'Figure 3-2 illustrates the 5G trust model for roaming.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 109, 'parent\_id': 'f79a12680dac9989cd20798158a41acd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '31b5098246b59c91314dd70fb27055c3', 'text': 'HPLMN and VPLMN are connected through Security Protection Proxy (SEPP) for control plane of interconnect network . . UDM - SEPP . = Source: 3GPP Trust model of roaming scenario', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 109, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '43c2a3a528655c6435f70b0027d2dfc4', 'text': 'Source: 3GPP Trust model of roaming scenario', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 109, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Header', 'element\_id': 'a0014939990515186611107ced286272', 'text': 'Figure 3-2 Trust Model for 5G Roaming Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 110, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '04c59d2a8eb2eaf079be3a895074f4ae', 'text': 'Integration of Non-3GPP Network to the 5G Core Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 110, 'parent\_id': 'a0014939990515186611107ced286272', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '20234f89d2b69140f0c2e6825985f5ce', 'text': "For non-3GPP access networks, 3GPP has introduced the Non-3GPP Interworking Function (N3IWF), which functions as a security gateway to allow the UE to access the 5G core over untrusted, non-3GPP networks through IP Security (IPsec) tunnels. Figure 3-3 illustrates the integration of the non-3GPP network to the 5G Core (5GC) network. The AMF terminates the Non-Access Stratum (NAS) security. The SEAF, which is co-located in the Phase 1 specification, holds the root key for the visited network. The Subscriber Identity De-Concealing Function (SIDF) decrypts the Subscription Concealed Identifier (SUCI) to reveal the Subscription Permanent Identifier (SUPI). When the home network public key is used for encryption of the SUPI, the SIDF uses the home network private key, which is securely stored in the home operator's network, to decrypt the SUCI.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 110, 'parent\_id': '04c59d2a8eb2eaf079be3a895074f4ae', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ff8d8925f10a46701359c5095cde4381', 'text': 'The Non-3GPP Interworking Function (N3IWF) provides IPsec between the UE and the N3IWF for both user plane and control plane traffic. N3IWF also helps with NAS signaling, initial registration, and authentication.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 110, 'parent\_id': '04c59d2a8eb2eaf079be3a895074f4ae', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '144071b031d2827b70dfc6012a78e8a3', 'text': 'Internet/ Data Network O N6 SMF N4 UPF 8B LT W — N SMF UDR 5GgNB 3GPP Access SCTP (NGAP) for P —» (D \\ Y1 Y2 N2 0 N3N6— 1§ Internet / Users & NWu WiFi/WLC | Data Network Devices Non-3GPP Access Psec for CP & UP GTP-Ufor UP', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 111, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '54992b14aa5e6c4d48ca5f5f9a01e028', 'text': 'UPF: User Plane Function UE: User Equipment SBI Service Based Interface SMF: Session Management Function WLC: Wireless LAN Controller SIDF: Subscriber Identty De-concealing Function AUSF; Authentication Server Function N3IWF: Non-3GPP Interworking Function CP: Control Plane ARPF: Authentication Credential Repository and Processing Function UP: User Plane UDR: Unified Data Repository SCTP: Stream Control Transmission Protocol NGAP: Next Generation Application Protocol GTP: GPRS Tunnelling Protocol', 'metadata': {'text\_as\_html': '<table><tbody><tr><td>UPF: User Plane Function</td><td>UE: User Equipment</td></tr><tr><td>SBI Service Based Interface</td><td>SMF: Session Management Function</td></tr><tr><td>WLC: Wireless LAN Controller</td><td>SIDF: Subscriber Identty De-concealing Function</td></tr><tr><td>N3IWF: Non-3GPP Interworking Function</td><td>AUSF; Authentication Server Function</td></tr><tr><td>CP: Control Plane</td><td>ARPF: Authentication Credential Repository and Processing Function</td></tr><tr><td>UP: User Plane</td><td>UDR: Unified Data Repository</td></tr><tr><td>SCTP: Stream Control Transmission Protocol</td><td>NGAP: Next Generation Application Protocol</td></tr><tr><td>GTP: GPRS Tunnelling Protocol</td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 111, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '18d2131e1e519492afd96f69acccdbc1', 'text': 'Figure 3-3 Integration of Non-3GPP Network to 5G Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 111, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b1e1df84dd19d60cfcd3de534f930782', 'text': 'Once authenticated, the N3IWF will also establish the user plane between the UE and the data network using the N3 interface between the N3IWF and the UPF.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 111, 'parent\_id': '18d2131e1e519492afd96f69acccdbc1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b71d131bf91ef9bddcb7b5e6cb7c7757', 'text': 'The reference points specific to non-3GPP access, as shown in Figure 3-3, are listed as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 111, 'parent\_id': '18d2131e1e519492afd96f69acccdbc1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd217ad69a4fe8f531bd37c32c82489cc', 'text': '• Y1: Reference point between the UE and the non-3GPP access', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 112, 'parent\_id': '18d2131e1e519492afd96f69acccdbc1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da193c36c964a2c384ddf99d0b0412c8', 'text': '• Y2: Reference point between the untrusted non-3GPP access and the N3IWF for the transport of NWu traffic', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 112, 'parent\_id': '18d2131e1e519492afd96f69acccdbc1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b5d5640bf08f89f5883adcb438945c5c', 'text': '• NWu: Reference point between the UE and N3IWF for establishing secure tunnel(s) between the UE and N3IWF so that control plane and user plane exchanged between the UE and the 5G Core Network are transferred securely over untrusted non-3GPP access', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 112, 'parent\_id': '18d2131e1e519492afd96f69acccdbc1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a290a21d46e714d8a5f6fc6b008f3fe8', 'text': 'Unified, Access-Agnostic, and Unified Authentication Framework', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 112, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd98a1cce40b31abbc2b96f60500bee10', 'text': "4G use cases were primarily voice and data for mobile subscribers, where the authentication was based on the 4G Evolved Packet System Authentication and Key Agreement (EPS-AKA) and required a physical or software Universal Subscriber Identity Module (USIM). 5G enables industry verticals to deploy new use cases—some of which require authentication with data networks (DNs) outside the service provider's domain. Such use cases might include non-3GPP-based devices.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 112, 'parent\_id': 'a290a21d46e714d8a5f6fc6b008f3fe8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9d8a2b1072744e538e781f7a0a9537df', 'text': "The 5G authentication framework allows both 3GPP and non-3GPP devices to authenticate and connect to your network. This is made possible due to the multiple authentication methods, such as 5G Authentication and Key Agreement (5G AKA), Extensible Authentication Protocol Authentication and Key Agreement (EAP-AKA'), and Extensible Authentication Protocol Transport Layer Security (EAP-TLS), as shown in Figure 3-4.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 112, 'parent\_id': 'a290a21d46e714d8a5f6fc6b008f3fe8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bb9bb8d373d1cec17d8cc544a2cfecc0', 'text': '4G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 113, 'parent\_id': 'a290a21d46e714d8a5f6fc6b008f3fe8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '55165bd870d7930d5ebff2f97d868821', 'text': '5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 113, 'parent\_id': 'a290a21d46e714d8a5f6fc6b008f3fe8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'caac807eb3206e92ec3dd8f68d2e110e', 'text': '5G allows multiple Authentication', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 113, 'parent\_id': 'a290a21d46e714d8a5f6fc6b008f3fe8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd54a20b1263dd89d55da28ea8aa81f88', 'text': 'mechanism Single Authentication + 5G-AKA-USIM mechanism + EAP-AKA"-USIM EPS-AKA - USIM + EAP-TLS - USIM/ Non-USIM - L— (4) L— (g) eNB gN\\B', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 113, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8bd60a5ee4303a6c6ad2f3b63ad4e284', 'text': 'USIM: Universal Subscriber Identity Module', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 113, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e303e128a4488e82025129b03b21a545', 'text': 'USIM: Universal Subscriber Identity Module EAP: Extensible Authentication Protocol AKA: Authentication and Key Agreement TLS: Transport Layer Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 113, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '061dfd096088e6b65b5d2e4ea19da44f', 'text': 'Figure 3-4 Comparison Between 4G and 5G Authentication Methods', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 113, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eec16dc3158f39b057b500a1c6f731ab', 'text': "EAP-AKA' and 5G AKA are mandatory 5G primary authentication methods, whereas EAP TLS is primarily seen in non-public network (NPN) deployments to enable the industry vertical/enterprise to reuse the existing security infrastructure for network access control for 5G devices. EAP TLS is also very useful for low-cost massive IoT (mIoT) deployments such as sensors and such, where SIM cards are usually not considered due to their prohibitive cost. These new authentication methods make 5G authentication access-layer agnostic.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 113, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d3b2d3deea9a37c1d8693829d55703a', 'text': 'To enable the unified authentication framework, 5G has introduced key Network Functions (NFs) such as Subscriber Identifier De-concealment Function (SIDF), Authentication Server Functions (AUSF), Unified Data Management (UDM), Security Anchor Function (SEAF) in the new 5G service-based architecture (SBA), and a new key hierarchy related to authentication in 5G System (5GS). Figure 3-5 illustrates the 5GS authentication key hierarchy.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 113, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b529a73fce3f2d1994730da30133d294', 'text': 'Network Side', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 114, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c0caf5f91a3b965c5eaa400ccf5411ee', 'text': 'UE Side', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 114, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '1a6fd467b161467a7c8d70ee98c1936c', 'text': 'UDMIARPF USIM UDMIARPF. = sasas ME HPLMN SGAKA | EAP-AKA Kausr K, K AUSF ME sssssbecaas PSP A SEAF ME AVF (o) () ® sening letwork um N3IWF ME ME | oNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 114, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '02924aa8e7bc4e5ad20001d52c1b6980', 'text': 'From: 3GPP TS 33.501', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 114, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'ListItem', 'element\_id': 'ea3912a4305d80e3e0c21e3d5631a2b1', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 114, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1f991a726474a80dd10388748c2905dc', 'text': 'Figure 3-5 5GS Authentication Key Hierarchy', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 114, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a434b1d2dd925f5dc52d07da89f9ddd3', 'text': 'As shown in Figure 3-5, the primary source of security context is the long-term secret key (K) provisioned in the USIM and the 5G core network, similar to the 4G key implementation. The differentiator here between 4G and 5G is the primary and secondary authentication. All devices have to perform primary authentication for accessing the mobile network services as well as secondary authentication to an external data network (DN), if so desired, by the external data network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 114, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5a56f47269a41852c930cd7678196c02', 'text': 'Another key area of enhancement is the UP integrity protection, which is another key enhancement that is valuable for the IoT-related use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 115, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7ce25762a33f0655c301ef1e680393d4', 'text': 'These security enhancements in 5G enable wider acceptability of 5G technology.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 115, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e6d35f5532e760697091c4204d3817ce', 'text': 'Use of Subscription Permanent Identifier (SUPI) and Subscription Concealed Identifier (SUCI)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 115, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4f43c6cbb91e5f7f5f864e9cc5f0d401', 'text': 'One of the risks was with the International Mobile Subscriber Identity (IMSI), which consists of 15 to 16 digits. This is the unique identity of the subscribers being occasionally sent in clear text while performing the Non-Access Stratum (NAS) procedures. The key risk here was the IMSI catcher, which is an eavesdropping device used for intercepting mobile phone traffic and tracking the location of the mobile phone users. The eavesdropping is performed by the IMSI catcher by mimicking a service provider cellular base station in order to force all nearby mobile phones and other cellular data devices to connect to it. Once these devices are connected, the IMSI catcher can force the UE to use no call encryption (A5/0 mode) or to use easily breakable encryption (A5/1 or A5/2 mode), making the call data easy to intercept and convert to audio, leading to a man-in-the-middle (MitM) attack scenario.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 115, 'parent\_id': 'e6d35f5532e760697091c4204d3817ce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cd31f0d0e51014bacbc1b25eb913939a', 'text': 'In 5G, privacy is achieved even before authentication and key agreement, by encrypting the SUPI before transmitting using a home network public key, which is stored in the USIM. 3GPP has specified SUCI, which replaces IMSI and T-IMSI for all air interface interactions, as shown in Figure 3-6.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 115, 'parent\_id': 'e6d35f5532e760697091c4204d3817ce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ac4723e7a236c63b68a2c69485a165b3', 'text': '4G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 116, 'parent\_id': 'e6d35f5532e760697091c4204d3817ce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2ea06685bc34347e7209b944d834dd05', 'text': '5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 116, 'parent\_id': 'e6d35f5532e760697091c4204d3817ce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'bec64e9c6f67bc376c5e6707f751d1a7', 'text': 'Initial messages with Initial messages with unique subscriber id info are now unique subscriber id in are sent in clear text ! encrypted in 5G ! = = L Sucl IMSI (A) SUPI == 4G Radio 5G Radio Node (eNB) Node', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 116, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0c39dc462c5ea19ca3fc53efcc2f237e', 'text': 'IMSI: International Mobile Subscriber Identity SUPI: Subscription Permanent Identifier SUC: Subscription Concealed Identifier', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 116, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cfd628e1efef6b29c5f8833808f0ccfd', 'text': 'Figure 3-6 Comparison of Subscriber Privacy Between 4G and 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 116, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '96889c08cb7bbfd7ed9dc649945291d4', 'text': 'Figure 3-7 illustrates the structure of the SUPI.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 116, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd618326a627a1ecbf72468b8972a755f', 'text': '| SUPI — > Max 15 -16 digits 2o0r3 |<— 3 digits —>| - \_,| digits', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 116, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '06015e349b1ce025443d3d10d65a9a19', 'text': 'Figure 3-7 SUPI Structure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 116, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8d20ccd64265915404016949d2f14dca', 'text': 'The SUPI contains sensitive subscriber and subscription information that is secured by the UE, which generates the SUCI, using a protection scheme based', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 116, 'parent\_id': '06015e349b1ce025443d3d10d65a9a19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3863bba323f40be5eaf5e3e512119a19', 'text': 'on Elliptic Curve Integrated Encryption Scheme (ECIES) profiles. Figure 3-8 illustrates the structure of the SUCI.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 117, 'parent\_id': '06015e349b1ce025443d3d10d65a9a19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'b5d27758cc35430296ba8044b186e31c', 'text': '—\_— i ——————————| Value range 0-7 0: IS NS 2:6Ll 3. GCl If SUPY s IMSI: MCC 4-T: spare +MNC 1-4 IFSUPHisNSI, GLI, digits Value range 0-15 GCl :string of Value range fSUPLis characters 0-255 S MSIN SUPIis S, GLI or GCl: sermname', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 117, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8c01a8691334acdffb873cce0995e92e', 'text': 'Figure 3-8 SUCI Structure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 117, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '800640c66aca5353c22929fee2081b58', 'text': 'As shown in Figure 3-8, the structure of the SUCI is composed of the following parts:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 117, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '89917fea5ba2d198cdee45a2e62ee244', 'text': '• SUPI type: The value range of the SUPI type is 0 to 7, as detailed next:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 117, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7bacf4a137b92021a86f153ebb270ee7', 'text': '• 0: International Mobile Subscriber Identity (IMSI)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 117, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '63e1eada52a114dfa848ac3eb0771f14', 'text': '• 1: Network Specific Identifier (NSI)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 117, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '93669f22523eaad8f908e507aeb4600b', 'text': '• 2: Global Line Identifier (GLI)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 117, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '35f934ce958a882095b09e127996459c', 'text': '• 3: Global Cable Identifier (GCI)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 117, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '226b6f5af6a35ce0d16e2308600f0a7c', 'text': '• 4–7: For future use', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 118, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '08e801cbe0f00663a2a97f7ed6fe1c35', 'text': '• Home network identifier: The value of the home network identifier will depend on the format of the SUPI type. If the SUPI is an IMSI, then the home network identifier will consist of a mobile country code (MCC) and mobile network code (MNC). If the SUPI type is NSI, GLI, or GCI, the home network identifier will consist of a string of characters that are variable in length, representing a domain name, such as user@serviceprovidername.com', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 118, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b74e03f8660cc9258885a39209686662', 'text': '• Routing indicator: The routing indicator consists of one to four decimal digits, provisioned in the Universal Subscriber Identity Module (USIM) by the home network service provider. This, along with the home network identifier, is used to route network signaling with the SUCI to the Authentication Server Function (AUSF) and Unified Data Management (UDM) in your 5G packet core to serve the subscriber user or device.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 118, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5cbd96270ab8aac64a3f68b986b739e0', 'text': '• Protection scheme identifier: The protection scheme identifier consists of a value in the range of 0 to 15, which indicates the non-null protection scheme specified by the home network service provider. Null scheme shall be used if the SUPI type is a GLI or GCI.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 118, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b41b920a3389f96d3e26975a56cb4cb', 'text': '• Home network public key identifier: The home network public key identifier represents the public key provisioned by the home network service provider or standalone non-public network (NPN), which is used to identify the key used for SUPI protection. Its value is in the range of 0 to 255.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 118, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f33303647f74a9997abde3d7bb8a25cf', 'text': '• Scheme output: The scheme output can be string of characters with variable length or hexadecimal digits, depending on the type of protection scheme used. If the SUPI type is IMSI, then the scheme output is the mobile subscriber identification number (MSIN), and if the SUPI type is network specific identifier, global line identifier, or global cable identifier, the scheme output is the username part of the network access identifier (NAI).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 118, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f732abc89765ba1784b150beae6194ce', 'text': 'These enhancements and evolution in authentication in 5G technology, specifically in non-AKA-based authentication mechanisms using EAP-TLS, allow industry verticals to adopt 5G deployments for non-public consumption. For service providers, this also means the enhanced capability to consume non- cellular IoT and IIoT devices as well as devices being served by non-3GPP', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 118, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ad90d0bae8817b210a92d6b023f1d64b', 'text': 'network access to register and connect to the 5GC using non-AKA protocols such as EAP-TLS and offering services for monetizing 5G deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 119, 'parent\_id': '8c01a8691334acdffb873cce0995e92e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b11bc784aa675d43a08528b64e5ce78b', 'text': 'Enhanced Inter-PLMN Interconnect Using Security Edge Protection Proxy (SEPP)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 119, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e0739baade5f3dd1b7958ae46c100837', 'text': 'In 4G, the Inter-PLMN Diameter messages can be exploited, leading to source address spoofing and other threats. 5G introduces SEPP to enhance the security of inter-PLMN interconnect, as discussed earlier in the section “5G Trust Model: Roaming.” Figure 3-9 compares the roaming security of 4G and 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 119, 'parent\_id': 'b11bc784aa675d43a08528b64e5ce78b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b88528c20e3c52526b4f1197b0431b27', 'text': '4G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 119, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '123d122c6b248cf0703dc5bcf57e4b9e', 'text': '56', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 119, 'parent\_id': 'b88528c20e3c52526b4f1197b0431b27', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '3cfef887f3fdba9fe9e70b190477251f', 'text': 'APIs are used in 5G with a defined network function Multiple protocols (Diameter, GTP, S87) called Secure edge Protection Proxy (SEPP) with many known vulnerabiltes !! ((A)) w W ((A>) Network when Network when Your home Your home you are foaming - you are foaming network - HPLMN VPLMN network - HPLMN VPLMN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 119, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b06659d5e06ea7290c10e0b50c073749', 'text': 'VPLMN: Visited Public Land Mobile Network HPLMN: Home Public Land Mobile Network PX: Internetwork Packet Exchange', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 119, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1627efa6bc0f2fc6cfbaf7463ea4e503', 'text': 'GTP: GPRS Tunneling Protocol GPRS: General Packet Radio Service §ST: Signalling System No. 7', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 119, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f7322ce97678504451cee1cdd6c08f16', 'text': 'Figure 3-9 Comparison Between 4G and 5G Roaming Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 119, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a31c78d4c31ae4c9302ddc9f4b5e54c7', 'text': 'SEPP implements application layer security for all the service layer information exchanged between two NFs across operator domains. This prevents IPX providers from reading sensitive information, such as', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 119, 'parent\_id': 'f7322ce97678504451cee1cdd6c08f16', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '295fdc0256af781d3ec7b2d44aa829e9', 'text': 'authentication vectors. SEPP can also detect any unauthorized message modifications, and it performs message source validation, message format verification, and topology hiding.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 120, 'parent\_id': 'f7322ce97678504451cee1cdd6c08f16', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9b99ca7554f9742ca27c1c54090e7b78', 'text': 'In additional to Transport Layer Security (TLS), Application Layer Security (ALS) is also needed to protect information elements (IEs) exchanged between Network Functions (NFs) of different operators.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 120, 'parent\_id': 'f7322ce97678504451cee1cdd6c08f16', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36c37239826cb52433638669cda35139', 'text': 'SEPP enforces inter-PLMN security on the N32 interface and is located in the perimeter of the PLMN for protecting inter-PLMN communications. The N32 interface consists of N32-c and N32-f. N32-c is the control plane, which is used by SEPP to negotiate the security capabilities. N32-f is the forwarding interface, also referred to as the end-to-end encrypted application interface. For N32-f, SEPP also provides encapsulation of HTTP/2 core signaling messages using JavaScript Object Signing and Encryption (JOSE) protection.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 120, 'parent\_id': 'f7322ce97678504451cee1cdd6c08f16', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0b5f2c3c375fc4bdf20cd505271231d1', 'text': 'Figure 3-10 illustrates the SEPP in a 5G interconnect domain.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 120, 'parent\_id': 'f7322ce97678504451cee1cdd6c08f16', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '13714fbf7ddeeae0baf72fafff404a21', 'text': 'ALS between SEPP - if negotiated by N32¢ T L N32- R L LLLLL L i i N32 N32-f N32 ((A>) L EPP ((A>) PX-A ¢ " PXB ¢ PLMN -A PLMN-B', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 121, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b243d4430a028e95c4d16640881b9bc5', 'text': 'Hop by Hop security can provided by IPsec or TLS VPN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 121, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '014891c28a30119f45412bc4e16f4d34', 'text': 'ALS: Application-Level Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 121, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '29420bb1f706a5abd5d017986163a1dc', 'text': 'TLS: Transport Layer Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 121, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '12b2cc41cc99561541ca5c7d93e3a808', 'text': 'SEPP: Security Edge Protection Proxy', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 121, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e7c3cddc7056467b98437c8e29983c8a', 'text': 'PLMN: Public Land Mobile Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 121, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4720bd66d9175a898e64bd79092391f7', 'text': 'PX: Internetwork Packet Exchange', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 121, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '69234e1b5d41bb96d6dcfeccad96526b', 'text': 'IPsec: Internet Protocol Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 121, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4067af618e3da9c209973d1a13aff2c6', 'text': 'Figure 3-10 SEPP in 5G Interconnect Domain', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 121, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8d6e48259e045a637817e615e120da95', 'text': 'Other Key Security Enhancements in Release 16', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 121, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0c4a7b4dd14d3234f5e355a0013cc18c', 'text': 'Rel-16 brought enhancements to a number of features. Each of these features is in the initial stages and will be subject to later modification or enhancement, over several years, by the means of change requests (CRs). The important Rel- 16 features are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 121, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dee0c3cd41a5f90a0c159efcc91308dd', 'text': '• Enhancement of ultra-reliable and low latency communications (URLLC)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 121, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58d00b3c675c3ea3ded46ef8139bf570', 'text': '• Support of LAN-type services', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 121, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bbd6cff8b329021f331f597e85f57a9e', 'text': '• Cellular Internet of Things (IoT)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c349f44c752e7ebe5970653d52d12664', 'text': '• Enhanced V2X support', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3c30ec7e12f1335f3e83d1ff6c4e41e3', 'text': '• API-related items', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4bb0a62ff22dd0711f120beb4ea2597f', 'text': '• Coexistence with non-3GPP systems', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'effe23701b1ed1d1d06f7dd766966797', 'text': '• Railways and maritime', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b09570964781f73b34dab4dc997d202b', 'text': '• Mission critical, public warning', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0231627532bd92380a6f49e4298dc80d', 'text': '• Conversational services, streaming, and TV', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a7f00972ca4befb6dcfd3e6aa87df96a', 'text': '• 5G location and positioning services', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '64a5f16e0d6ac4dd89d84aec9ee09d6b', 'text': '• User identities, authentication, multi-device', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2331a8c6782765e866ec392ae2c160bd', 'text': '• Network slicing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b93d1eba316ef0aa5ee101ff8708d70e', 'text': '• UE radio capability signaling optimization', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c2f8d057a308647c834b266de07c3790', 'text': 'The list of all the features introduced in Rel-16, including the aforementioned ones, is provided in the 3GPP document TR 21.916, “Summary of Rel-16 Work Items.” Some of these new features also bring in enhanced security, which is discussed further in the following section.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'parent\_id': '8d6e48259e045a637817e615e120da95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '75dd18ecbcbe023edd05418a00da1ec0', 'text': 'Security Enhancements in Northbound API-Related Items', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '812989cfcd2651764c152497c8f35bb1', 'text': 'While a basic Common API Framework (CAPIF) is made available in 3GPP Rel-15, there are several enhancements that are considered for developing eCAPIF in Rel-16, which introduces key features such as support for stronger integrations with third-party domains, as shown in the Figure 3-11. Key enhancements are based on the enhanced interconnection between two CAPIF providers, support for distributed deployments, and closer integration between third-party API providers and the CAPIF framework.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 122, 'parent\_id': '75dd18ecbcbe023edd05418a00da1ec0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'e0cd89ad9ce84fcae406bd6bed160651', 'text': 'Web Critical 39 party Virtual Network Industry and Infrastructure Application Enterprise Verticals Services Operator developers Q\_p oo ( A)) A g1 o i ................ \* FEIEUTI S i i - i - Third Party Application Rel-16 CAPIF S enhancements to secure Northbound API 5G Core Service Based Architecture (SBA) Service Based Interface (SBI) - ..... T 1 SMF E AMF 1i RF LI B I |', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 123, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5e8902c144e2a9e45765b7b2ef499fb1', 'text': 'Figure 3-11 3GPP Rel-16 Enhancement for Better Third-Party Domain Support for CAPIF', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 123, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e5572acd3455ce38b44b7b3b6d476755', 'text': 'The architecture functional model supports multiple API providers (within and outside the PLMN trust domain), where CAPIF-3, CAPIF-4, and CAPIF-5', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 123, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bfec988310c7b56d4d23ae7ba1f0dd28', 'text': 'were enhanced as CAPIF-3e, CAPIF-4e, and CAPIF-5e, respectively, to enable the API-exposing function, the API publishing function, and the API management function of the API provider domain within the third-party trust domain interaction. The API-exposing function within the PLMN trust domain also interacts with the API-exposing function in the third-party trust domain via CAPIF-7e, as illustrated in Figure 3-12.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 124, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'b950ba4a02a63eed5472deee110b4413', 'text': 'API Invoker 1 [ T T T PR RS ——— T TLLLLrrrrrTrrTrT API CAPIF ; Invoker 3 APIF-1e CAPIF-2 IF 28 Service APIs API Exposing | CAPIF-3 Function % Zz-3A\\avO 4 CAPIF-4 API Publishing A\\ " Function ) 3¢ Party CAPIF-5 W Trust Domain - APIManagement Function YSTSTSTeppip \'y Spiyipupny pRpepey— CAPIF core ! APl provider domain L L L L Service APIs function CAPIF-3¢ API Exposing Function E CAPIF-4e API Publishing Function CAPIF-5¢ ; PLMN Trust Domain | E FesEssssssssssssssssssssssssssssssssssssssssssssssaad | | : API provider domain 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 125, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bf7e1a1caa96af9b562732e34fe661f5', 'text': 'API Invoker 1', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 125, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cafe9799e8d339cd39aa48d3cdab4198', 'text': 'Figure 3-12 3GPP Rel-16 CAPIF Security Functional Model', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 125, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6a5d2e2a144a2167530c3b88b633cb55', 'text': 'The key security enhancements for CAPIF in Rel-16, as specified in 3GPP TS33.122, are further detailed next:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 125, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '96f7175e99e0a88a87263ab2e0f514ae', 'text': '• Rel-16 introduces API topology hiding. When topology hiding is enabled, the CAPIF core function shall respond to service API discovery requests with AEF information, which exposes the service API and acts as a topology-hiding entity.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 126, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a53f80393013a00c67ed7a8b2f96036d', 'text': '• Mandatory support of TLS for integrity protection, replay protection, and confidentiality protection for CAPIF-1e/2e/7e interface.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 126, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4d7a3ab5b2e311e3443f56d73eef907d', 'text': '• The API invoker and the API-exposing function using CAPIF-2e will establish a dedicated secure session using a TLS connection based on one of the following methods.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 126, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '31fa6aecd28d9df0e7c0eedaef4ceecd', 'text': '• TLS-PSK: TLS-PSK is one of the TLS key exchange methods that uses symmetric keys, shared in advance among the communicating parties, to establish a TLS connection. This method is generally used in a closed network environment to avoid the need for public key operations.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 126, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1796a32f906f02ec436799f0eaadacc4', 'text': '• TLS-PKI: TLS-PSK is one of the TLS key exchange methods that uses keypairs—public key and private key—to establish a TLS connection. Public keys can only encrypt and cannot be used for decryption. Since the message is encrypted using a given public key, it can only be decrypted by the matching private key. This establishes the ownership of the private and public key, ensuring the message is only read by the approved parties. This is one of the most scalable and widely used methods to establish TLS by service providers today.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 126, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e3981b14109c39c234ea2a8dec6c31cc', 'text': '• TLS with OAuth token: In this method, once the TLS is successfully established, the OAuth 2.0 protocol flow is carried out in Figure 3-13. The OAuth protocol flow is illustrated in the Figure 3-13.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 126, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'bfd9488ca3400b7e1534c02e40bef530', 'text': '— A Authorization Request —» Resource Owner <+— B Authorization Grant — C: Authorization Grant — Authorization Client Server < D : Access Token — E : Access Token Resource Server < F: Protected Resource', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 127, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '81927f7d063df483d1030d69c04e4d0f', 'text': 'Figure 3-13 OAuth Protocol Flow', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 127, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '507eea2db1b0732c82411cc1ed83293e', 'text': 'The OAuth flow is as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 127, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f6e75ef23b4900669cbb2a9a3c06ef8c', 'text': 'A. The client requests authorization from the resource owner (directly or via the authorization server).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 127, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7fc2d92985d720ac1e06cdcd7278c56c', 'text': "B. The client receives an authorization grant (a credential representing the resource owner's authorization).", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 127, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8c1f3e0475f25ff55469edc23c7cc11d', 'text': 'C. The client requests an access token by authenticating with the authorization server and presenting the authorization grant.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 127, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bac621023b7576c82bcf71fa9962ff46', 'text': 'D. The authorization server authenticates the client and validates the authorization grant, and, if valid, issues an access token.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 127, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '11356770840b6eaedb6d243e268d9a90', 'text': 'E. The client requests the protected resource from the resource server and authenticates by presenting the access token.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 127, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eda4893063885d14bdb9a4fd32742dae', 'text': 'F. The resource server validates the access token and, if valid, serves the request.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 128, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8abeba5c9bddcd5ecf02d22aa00d2494', 'text': "After successful establishment of TLS on the CAPIF-2e reference point, the API-exposing function shall authorize the API invoker's service API invocation request based on authorization information obtained from the CAPIF core function. The same method will also be used by the CAPIF 7e interface, which provides communication between API-exposing functions in the PLMN trust domain and third-party trust domain.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 128, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7bbe1ee2f5a26064a5135800ac2eaa6b', 'text': 'CAPIF-3e/4e/5e are secured using TLS and IPsec using SecGW.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 128, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '719cf27cb6ac1996c765b7f8a46cfd88', 'text': 'Mission-Critical Services', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 128, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd87e893b44cb7692c42fb0ead374cd8e', 'text': 'Security enhancements for mission-critical (MC) services provide the confidentiality, integrity, user authentication, service authorization, and overall security architecture for the Release 16 mission-critical features, including MC Push to Talk (MCPTT), MCVideo, MCData, MC Location, MC Interworking, MC Interconnection, and MC Railway.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 128, 'parent\_id': '719cf27cb6ac1996c765b7f8a46cfd88', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a4b4753b63003098188c0c7aae8075fb', 'text': 'Release 16 expands on the mission-critical security architecture already defined in previous releases, along with various mission-critical security clarifications and corrections. In this release, mission-critical security, as defined in 3GPP TS 33.180, adds user service authorization for the mission- critical location service. Similar to user service authorization for the other MC services, an appropriately scoped access token is obtained from the identity management server that permits only authorized users to access the MC location service.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 128, 'parent\_id': '719cf27cb6ac1996c765b7f8a46cfd88', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '703a47d0813e9064f17cc3018e44af08', 'text': 'MCData payload protection is enhanced to support separate algorithm types for the MCData payload field, which allows the architecture to meet varying security needs of the mission-critical operator for both on- and off-network MCData operational scenarios.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 128, 'parent\_id': '719cf27cb6ac1996c765b7f8a46cfd88', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '94b04dc03446a294e4286a4587571070', 'text': 'Within a mission-critical system, the signaling plane should be secured using IPsec for SIP signaling and TLS for HTTP signaling, as shown in Figure 3-14.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 128, 'parent\_id': '719cf27cb6ac1996c765b7f8a46cfd88', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '80ddee3bc0256e227ad1be968e69dc7f', 'text': 'HTTP Proxy SIP Core i HTTP and SIP HTTP 8P (IPsec) Signalling Signalling MC MC Network | Network (TLS) Psec) Element Element', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 129, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b15c226396f4574d96c30abcb07d773a', 'text': 'MC: Mission Critical', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 129, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4ba90cfb0573f5e972b150aa9580ef27', 'text': 'SIP: Session Intiation Protocol HTTP: Hypertext Transfer Protocol', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 129, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0634392bc7e4eabaa1bf2adf0b8b136d', 'text': 'TLS: Transport Layer Security IPsec: Internet Protocol Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 129, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '27a4b7ed5f10dc668586ea88dbe54a21', 'text': 'Figure 3-14 Signaling Plane Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 129, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e54136bddfdb2cb8a38c126678eaaa7a', 'text': 'Application plane signaling security protects application signaling between the MC client and the MCX server. Initial key distribution for application signaling is performed by sending a client-server key (CSK) from the MC client to the MCX server over the SIP interface. The key is secured using the identity key material provisioned by the key management server. Following initial key distribution, the MCX server may perform a “key download” procedure to update key material as well as to key the client to allow multicast signaling to be protected, as illustrated in Figure 3-15.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 129, 'parent\_id': '27a4b7ed5f10dc668586ea88dbe54a21', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '6f6f321a979e47533b6bda9730d91208', 'text': '[y ——— MCX Server MCX Server e e | | ! [nitial ‘Key download’ Key Application Management Client-Server For key update plane signalling Server Keying and multicast (XML, RTCP, keying MCData : signalling) i Emeem .- MC Client MC Client MC: Mission Critical XML: Session Initiation Protocol RTCP: Real Time Control Protocol', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 130, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ae550ec752426845c0e6ce0205d89ea0', 'text': 'MC: Mission Critical', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 130, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed24830057c4a4dece6b306b9e1b56a5', 'text': 'XML: Session Initiation Protocol', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 130, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a17849b28118dab393f4d71b4a31b7d', 'text': 'RTCP: Real Time Control Protocol', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 130, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '08fac12fded878b9d0d6fc554ba7fc91', 'text': 'Figure 3-15 Application Plane Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 130, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b8797e40461fe30ea15e81f480a3f7d9', 'text': 'Rel-16 further introduces enhanced security for interconnection, which now combines the MC gateway, Interconnection Signaling (IS) proxy, and HTTP proxy to provide topology hiding, HTTP protection, and signaling protection for inter-domain MCPTT, MCData, and MCVideo communications between two disparate mission-critical systems for a complete interconnection security solution, as illustrated in Figure 3-16.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 130, 'parent\_id': '08fac12fded878b9d0d6fc554ba7fc91', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '3115a05be82e51fdc317d94fda650a62', 'text': '- Mission Critical Domain Config Group Mgmt Mgmt Server Server [ ey ——— [ Signalling Proxy ! Signalling Security l MC: Mission Critical PTT: Push to Talk Mgmt: Management External entities CS: Client Signalling IS: Interconnection Signalling', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 131, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '10e15c41cb665fe308e30e2b3c3c5ad1', 'text': 'Mission Critical Domain', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 131, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f2ac97bd4957252fc2903e72ed976fa9', 'text': 'Figure 3-16 Interconnection Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 131, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b87688242da37374d0845c6370226eb1', 'text': 'Service Enabler Architecture Layer (SEAL) for Verticals', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 131, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fab34749952a14d7d3475229b5f06b5f', 'text': 'Similar to the Common Functional Architecture (CFA) for mission-critical services, a set of common capabilities can be utilized by V2X and potentially by multiple vertical industry applications, referred to as the vertical applications layer (VAL) in this section. In Rel-16, this set of common capabilities is developed as a service enabler architecture layer (SEAL) over 3GPP networks and is specified in Stage 2 SEAL in 3GPP TS 23.434. The key security enhancements specified in TS 33.434 are further discussed in this section.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 132, 'parent\_id': 'b87688242da37374d0845c6370226eb1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '854807b5bf8063c5ed65cfee113cd1e0', 'text': 'Figure 3-17 illustrates the on-network functional model of SEAL.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 132, 'parent\_id': 'b87688242da37374d0845c6370226eb1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'beb6fce55a98c21e91565a9999b370f8', 'text': 'VALW VAL Clients VAL Server VAL 3GPP Network SEALC SEALS sssssscssansssshasassasasnsadeacancnnananefensanancacananshessnsnasasnsnncanadeacanannanannannscacashacacanannanananananns System SEAL SEAL-W SEAL Clients SEAL Servers VAL: Vertical Applications Layer SEAL: Service Enabler Architectural Layer 3GPP: 3¢ Generation Partnership Project', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 132, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '071f47724976608b1c859d227a101b83', 'text': 'VAL: Vertical Applications Layer SEAL: Service Enabler Architectural Layer 3GPP: 3¢ Generation Partnership Project', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 132, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6bd17ae4106bddfd137aec684835cfaa', 'text': 'VAL: Vertical Applications Layer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 132, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8fc1d7ff1d42fef88fab0dada8e68c59', 'text': 'Figure 3-17 SEAL On-Network Functional Model', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 132, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ac421841a5c621a31e806e0351a00f67', 'text': 'The application plane interfaces, such as VAL-UU and SEAL-UU, should be secured by TLS and IPsec mechanisms.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 133, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '60c0b5edfb4fcddfece8da0e9fdb6e69', 'text': 'The SEAL Identity Management Server (SIM-S) and the SEAL Identity Management Client (SIM-C) provide the endpoints for VAL user authentication using the IM-UU reference point, as shown in Figure 3-18. IM- UU supports OpenID Connect 1.0 and OAuth 2.0 for VAL user authentication.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 133, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'bd85099d992a6ab04d1fd097b1fca82d', 'text': 'SEAL Identity Management IM-UU SEAL Identity Management Server Client (SIN-S) (SIM-C)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 133, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '16165a4396f27304aada7b4d011ed1ea', 'text': 'Figure 3-18 SEAL Identity Management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 133, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '307fbc71bd3dcd15f7511d69ef381c35', 'text': 'Similar to the introduction of signaling proxy functions in the mission-critical services, the SIP core and HTTP proxy layers are introduced for SEAL deployments for securing SEAL signaling control plane messages, as shown in Figure 3-19. The SIP core provides security functions such as authentication and security to the service layer, overload control, and session management.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 133, 'parent\_id': '16165a4396f27304aada7b4d011ed1ea', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f391a04a4b2afc80f0018c9ea7d71bca', 'text': 'Toother SEAL system ] MAf SPDB | SIPcore SIP-1 Signalling — user agent Prox Diameter — AMA2 proxy SIP-2 SIPAS 3GPP Network SEAL Client System HTTP HTTP-2 Server HTTP- HTTP-A HTTP Client SEAL HTTP-3 Server To other SEAL system AAA: Authentication, Authorization, and Accounting SEAL: Service Enabler Architectural Layer SIP: Session Initiation Protocol DB: Database HTTP: Hypertext Transfer Protocol SIP AS: SIP Application Server 3GPP: 3 Gengration Partnership Projgct', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 134, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a4af02dbf02dfc579a1af7f5c9bf67f8', 'text': 'AAA: Authentication, Authorization, and Accounting SIP: Session Initiation Protocol HTTP: Hypertext Transfer Protocol 3GPP: 3 Gengration Partnership Projgct', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 134, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b6d3732c557af28564326e83e19983bd', 'text': 'SEAL: Service Enabler Architectural Layer DB: Database SIP AS: SIP Application Server', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 134, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '50c9221b083263f676252d8a45179ead', 'text': 'HTTP: Hypertext Transfer Protocol 3GPP: 3 Gengration Partnership Projgct', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 134, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dfee608632a4ca8eff2d2a4c4c8e9787', 'text': 'Figure 3-19 SEAL Signaling Control Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 134, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5421260459140729a21fccaadbffe794', 'text': 'The HTTP-1 reference point exists between the VAL UE and the HTTP proxy. The HTTP-2 reference point exists between the HTTP proxy and HTTP server. The HTTP-3 reference point exists between the HTTP proxies in different networks. The HTTP interfaces shall be protected using TLS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 134, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5fe1a59294519816507a3be4822735a1', 'text': 'The HTTP proxy acts as a proxy for hypertext transactions between the HTTP client and one or more HTTP servers. The HTTP proxy terminates a TLS session on HTTP-1 with the HTTP client of the VAL UE, allowing the HTTP client to establish a single TLS session for hypertext transactions with multiple HTTP servers that are reachable by the HTTP proxy.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 135, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '56c365430c6a1ebcb3f723e37bba7418', 'text': 'Enhancements for User Identities and Authentication in Slicing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 135, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f1cca0d154062a3c59ecabb9137d8ac5', 'text': 'This feature allows the use of a user identifier, which is independent of existing identifiers relating to a 3GPP subscription or UE, for network slice-specific authentication and authorization (NSSAA).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 135, 'parent\_id': '56c365430c6a1ebcb3f723e37bba7418', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '54f96d239a4704622300a2ee796e1d60', 'text': 'In addition to 3GPP-defined network slice selection and authorization, it also defines the interworking of the 3GPP system with an external entity to authenticate and authorize user to access a specific slice. The actual identity provisioning service with creation, management, and authentication of identities is not specified by 3GPP.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 135, 'parent\_id': '56c365430c6a1ebcb3f723e37bba7418', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2019b77ef0b00cc0a665a8a7c8c3174d', 'text': 'Rel-15 network slice selection is based on the NSSAI, which consists of one or more S-NSSAIs. In Rel-16 feature enhancements, subscription information allows the indication of which S-NSSAIs are subject to network slice-specific authentication and authorization (NSSAA). For those S-NSSAIs, the AMF invokes an EAP-based network slice-specific authentication procedure in which the AUSF exchanges AAA protocol messages with a potentially external AAA server (AAA-S) via an optional AAA proxy (AAA-P) to authenticate and authorize the UE for the network slice. Depending on the result of the procedure, the UE is either authorized for a network slice, re-allocated to a different one, or deregistered. A re-authentication and re-authorization procedure may be triggered by the AAA server at any time.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 135, 'parent\_id': '56c365430c6a1ebcb3f723e37bba7418', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7513187eee788df85e04956f479b5d85', 'text': 'Security Challenges in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 135, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ce3ba4b3ebf0b66f38b292315545959b', 'text': '3GPP specifies some preventative measures to limit the impact of known threats; however, the adoption of new use cases that require integration with existing technologies from industry verticals, the introduction of new deployment models, and the changes in the 5G architecture, such as the use of APIs in service-based architecture (SBA) and NSaaS, introduces potential new threats for the industry to manage. Adoption of new deployment methods and', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 135, 'parent\_id': '7513187eee788df85e04956f479b5d85', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0dcd049beec42d7f99aa897d74ecf2a2', 'text': 'technologies, such as public cloud deployment models, integration with third- party multi-access edge compute (MEC) applications, and network slicing, will require new security controls to be implemented, other than those introduced by 3GPP.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 136, 'parent\_id': '7513187eee788df85e04956f479b5d85', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6fe9c60686c43bd07cc1ebcd7f7f4f93', 'text': '5G enables openness and flexible deployments due to the use of cloud-native principles, allowing 5GC network functions to be built using polyglot architectures with open source software and implementation of SBA, which uses API-based communication between the 5GC control plane functions. Figure 3-20 illustrates some of the key challenges in 5G technologies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 136, 'parent\_id': '7513187eee788df85e04956f479b5d85', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'e68ac6e78e94616d945ef71f08ab89ee', 'text': "LloT8N \\ ’ omn- Perimeter less deployments Virtualized and Polyglot - architecture Contaner 1 PN I Cloud ¥a : crosenvice 2 oo B I w 'l-\\‘] 3 Container 2 R R — \\S Iz fosendoe 4 & Mitoservices Mw:'nsv'wcuD [ 0 dpoyedn N depyedn NN ontangr Traditional hybrid cloud [+ ] —\_— - = ————— S . \\, e - TSR ——— T —— — | LR —— ———— 0 Microservices Weak inbuilt 5G components can be deployed on- Virtualized 5G components use open- security in loT source programs which introduce premises and in the cloud, this breaks the devices, peer to concept of perimeter-based deployments. vulnerabilities. We didn't have to peer attacks, V2X worry ahout his in 4G. Use cases We didn’t have to worry about this is 4G", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 136, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '14278153b0defabdcafda6a948d66a1e', 'text': 'Figure 3-20 Key Challenges in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 136, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6424fcbe2e9f3f4e433f9cd529005a68', 'text': 'The sections that follow discuss the key challenges shown in Figure 3-20.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 136, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c7246566fde269461f0b612b9277c8e4', 'text': 'IoT and M2M', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 136, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b03a3965309a243457df0642e7c6b8a3', 'text': '5G technology will also usher in new connected experiences for users with the help of massive IoT devices and partnerships with third-party companies to allow services and experiences to be delivered seamlessly. For example, in the auto industry, 5G combined with machine learning–driven algorithms will provide information on traffic and accidents as well as process peer-to-peer traffic between pedestrian traffic lights and vehicles in use cases such as vehicle-to-everything (V2X). Distributed denial of service (DDoS) in these use cases is a very critical part of the 5G threat surface.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 137, 'parent\_id': 'c7246566fde269461f0b612b9277c8e4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '50b793d0b5f744762d6d4f6830bb0c9c', 'text': "IoT has been around for quite some time, and some use cases such as wireless point-of-sale (PoS) terminals use 2G in many countries where 2G coverage is prominent. But when we speak about IoT in relation to 5G deployment, it refers to IoT devices of various types. Some IoT devices are not smart devices, and they just send information back to the network in bursts and don't process data or do any analytics within the IoT device itself. Such devices do not have the capability to protect themselves from tampering or any bot taking them over. Some IoT devices are semi-smart and have the intelligence to filter certain data and perform some high-level analysis; however, even these devices have very little or no security, as they were made to fulfill a certain use case with easy and flexible deployment without focusing on the security. True smart IoT devices will help fulfill the critical infrastructure use cases and have the capability to secure themselves and provide security during the information exchange with the management servers. The main threats for IoT and machine- to-machine (M2M) deployments in 5G are related to hardware and software supply chain vulnerabilities and application-level threats, which require more security focus than 3GPP-specified enhancements to 5G.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 137, 'parent\_id': 'c7246566fde269461f0b612b9277c8e4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '903ee370210fda784e0283848043b098', 'text': 'Chapter 8, “Securing Massive IoT Deployments in 5G”, and Chapter 9,', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 137, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f77ba7c0652b102ae4f5a78406e8f22a', 'text': 'Chapter 8, “Securing Massive IoT Deployments in 5G”, and Chapter 9, “Securing 5G Use Cases,” cover the topic of IoT and M2M threat surfaces in more detail. You will also see supply chain threat mitigation covered for domains such as RANs, transport, MEC, and virtualized 5G Core throughout this book, as it is a very extensive and critical part of the end-to-end 5G security architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 137, 'parent\_id': '903ee370210fda784e0283848043b098', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'aef442baeb4a8e9709a1283fb707d2dd', 'text': 'Perimeter less Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 137, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0cb3115fe9c0dcd9583a8cb39ee009d1', 'text': '5G introduces network decomposition and disaggregation into software and hardware as well as infrastructure convergence, which underpins the emergence of edge computing network infrastructure or MEC. 5G edge computing use cases are driven by the need to optimize infrastructure through', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 137, 'parent\_id': 'aef442baeb4a8e9709a1283fb707d2dd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ec9aa49c7c8eb96450458586535b0b91', 'text': 'offloading, better radio, and more bandwidth to fixed and mobile subscribers. New architectures such as network slicing enable multiplexing of this disaggregated and decomposed infrastructure and help provide isolated end-to- end networks tailored to fulfill diverse requirements being requested by new 5G use cases. The need for low-latency use cases such as URLLC, which is one of several different types of use cases supported by 5G, requires user plane distribution. Certain 5G-specific applications and the user plane need to be deployed in the enterprise network for enterprise-level 5G services for NPN deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 138, 'parent\_id': 'aef442baeb4a8e9709a1283fb707d2dd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '34ddbb46e1b180bba054058a6589a6c7', 'text': 'The key threats in MEC deployments are mainly due to improper implementation of APIs, the use of third-party applications being developed without security in mind, insufficient testing of software code, malicious/rogue MEC deployments, API-based attacks, insufficient segmentation, and improper access controls on MEC deployed on enterprise premises. MEC deployments with third-party workloads are specifically prone to malicious code injection attacks due to weak inherent security implementation in the software development stage, leading to data exfiltration and other risks during live deployments. Such deployments using third-party workloads should be secured with multi-layered security controls, which is explained in detail in Chapter 5, “Securing MEC Deployments in 5G.”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 138, 'parent\_id': 'aef442baeb4a8e9709a1283fb707d2dd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '59c6b993a0716a52a5c1f6653539dbd6', 'text': 'Deploying 5G Network Functions (NFs) in the public cloud brings in the shared responsibility model, where the cloud service provider and the 5G mobile network service providers or industry verticals deploying 5G have to share the responsibility of securing the workloads and the communication of the workloads. In the shared security model, you are responsible for part of the security when moving the workloads, such as 5G Cloud Native Functions and third-party MEC applications, to the cloud. To fulfill the shared security model, you need security controls other than what is specified by 3GPP, such as ensuring that you and the 5G vendor follow strict CI/CD procedures, employing dynamic and automated vulnerability management to secure the runtime environment, ensuring the implementation of the correct security policies when new instances of 5G NF are instantiated by the orchestration layer, and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 138, 'parent\_id': 'aef442baeb4a8e9709a1283fb707d2dd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7d40ce47b1930f7226d80067ccad9608', 'text': 'Virtualized Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 138, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b490fc69b198401d63115986c73f6537', 'text': 'Virtualization and cloud-native architecture deployment for 5G are some of the key concerns for service providers. Although virtualization has been around for', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 138, 'parent\_id': '7d40ce47b1930f7226d80067ccad9608', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cca70ce81127aa763d6c11ccb0768963', 'text': 'a while, and you have seen Virtualized Network Functions based on virtual machines in 4G, the container-based deployment model consisting of 5G Cloud-Native Functions (CNFs) is a fresh approach. Apart from the known vulnerabilities in the open source components used to develop the 5G CNFs, most CNF threats are actually unknown, which is riskier. The deployment model of CNFs in the public and private cloud brings in another known yet widespread problem of inconsistent and improper access control permissions putting sensitive information at risk.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 139, 'parent\_id': '7d40ce47b1930f7226d80067ccad9608', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5df9acf53023ef3b147aa0ea41cd2a8d', 'text': 'The adoption of CNF brings in a whole new ecosystem, such as new methods of development and deployment. One example is the software development method, which follows polyglot architectures. This means that the 5G Network Functions (NFs) are now developed using any open source programming language (Golang, Python and so on) and will follow the development model used by various enterprise applications. While this opens the door to a range of applications and enables critical use cases, it also brings in the need to identify, track, and apply a robust vulnerability and patch management system to the 5G ecosystem. In previous generations, the software was vendor proprietary, and the vulnerabilities were tracked and immediately acted upon by the vendor, which knew the ecosystem extremely well. In polyglot architectures, this becomes a double-edged sword. While the vulnerabilities and bugs are identified by the open source communities, polyglot architectures are also exploited quite easily by the attackers before they are patched or a workaround is suggested. The deployment model also brings in a new threat surface linked to supply chain vulnerabilities, as the method of downloading the image from the repository and deploying it should follow strict best practices, without which you will be essentially compromising your entire network and subscriber-sensitive information.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 139, 'parent\_id': '7d40ce47b1930f7226d80067ccad9608', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '25093757638f602b288ed6e9b66453ca', 'text': 'The adoptability of 5G CNF and the new SBA, which uses API-based communications, introduces a host of other threat surfaces that are not mitigated by security enhancements brought in by 3GPP for 5G technology. API-based SBA is fragile in nature, as it is prone to weak implementation by developers, and there are many known vulnerabilities in the API web servers today that can be exploited by attackers to gain access to critical 5G infrastructures and exfiltrate sensitive information—or worse, cause a denial of service (DoS) attack that potentially leads to a loss of revenue.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 139, 'parent\_id': '7d40ce47b1930f7226d80067ccad9608', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9a0ad9c0039620cb8e96f6e7be0a485e', 'text': 'Securing virtualized deployments in 5G is further discussed in detail in Chapter 6, “Securing Virtualized 5G Core Deployments.”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 139, 'parent\_id': '7d40ce47b1930f7226d80067ccad9608', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c6731ae8f207a6a00324a4475eed35f2', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '62d856cadcd4d169d398726e0c4f3962', 'text': '5G technology will introduce advances throughout the network architecture, such as decomposition of RAN, utilizing APIs, container-based 5G Cloud- Native Functions, and network slicing, to name a few. These technological advancements, while allowing new capabilities, also expand the threat surface, opening the door to adversaries trying to infiltrate the network. Figure 3-21 illustrates the key end-to-end threat surface in 5G deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': 'c6731ae8f207a6a00324a4475eed35f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ea4a7d66f8953b00827b460b9947ea77', 'text': '— i ((A) <>UpF E —— fils O v cU & Third Party Applications & Dirgct Internet Access — ((A)) 13301] — o OB — ~OF - \\ ;hxrd Party Applica — v MEC Appln NRF, AMF.... SMF Direct Internet Ac W e i RRU [ —— g T [—— | / UPF 5CP CM, PM,FM f— % B J— A — <> UPF| i S — \\ \\ 56C MEC gNB freals Air Inferface Threats RAN & Fronthaul Threats MEC & Backhaul Threals 5G Packet Core & OAM Threats SGi/N6 ¢ Threals Mith attack DDoS attacks Virualisation Rogue Nodes S Jamming Rogue Applications on Lawful Intercept Vulnerabilies Orchestration Vulnerabilties loT Core 1Hacks programmable routers SON Vulnerabilties Improper Access Control VAS intey ampering Insecure $1, X2 AP Vulnerabilties Network Slice Vulnerabilties App serve usceptibilty Insecure Xx, Xn Insecure Sx API vulnerabilties Applicatio', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '37036eeff29534509f480c34cc4e7e82', 'text': 'freals Air Inferface Threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '264ff8f4505d815f6060bc0e542ce024', 'text': 'RAN & Fronthaul Threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9c6b8efa8b7c965fd2ddb15389f68f0c', 'text': 'MEC & Backhaul Threals', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '51499d75eaaa81cfc113107637dcb888', 'text': '5G Packet Core & OAM Threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0d6791876d772910cd5da8ca626c318b', 'text': 'freals', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8484fea6e756ea2901d5cf8caeb9e59b', 'text': 'Mith attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '0d6791876d772910cd5da8ca626c318b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'df8f865526694ac9b26892ec7c37be65', 'text': 'Rogue Nodes', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '0d6791876d772910cd5da8ca626c318b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '92dc3287b158539d4b2d22b5d87cd2fa', 'text': 'Virualisation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '0d6791876d772910cd5da8ca626c318b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '786002fa76029bad3464ec1b2fd1da02', 'text': 'S', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '717447c709bddf457b34f7bc9f8d6bad', 'text': 'Jamming', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e24bda3660c657e7a737b2d5d30ce12a', 'text': 'Lawful Intercept Vulnerabilies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '462c37ed338480d7ce40820a2ee0ac50', 'text': 'Orchestration Vulnerabilties', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4ff91672d44289db2cc65add5d17b126', 'text': '1Hacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7ec085c65907c3734f0fb18b21db004e', 'text': 'programmable routers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '758016a46e6a574003942d0a2c1f30dc', 'text': 'SON Vulnerabilties', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a69c78ba6677c8e07a81a8dad4a3d977', 'text': 'Improper Access Control', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6dab664187da08ea25a3249bbf420852', 'text': 'Insecure $1, X2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd992e50254a3375343e3c5570aa819f5', 'text': 'AP Vulnerabilties', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2fa06fcf713f8bbac77797cf23da207c', 'text': 'Network Slice Vulnerabilties', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bf9c28bd14a6748e294f9ee94bb0648d', 'text': 'Insecure Xx, Xn', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b39e73e2a570f34ba970f51d1fc6226e', 'text': 'Insecure Sx', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '42a40122271cbd7d0959c6037fecdff1', 'text': 'API vulnerabilties', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '17f08d0268cfd8e81e51187b0789a9cd', 'text': 'Figure 3-21 End-to-End Threat Surface in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '577952e12c574039c4ba5612963a2b2b', 'text': 'SGi/N6 ¢', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f84123ade8783d6064c7180543e8da4e', 'text': 'Threals', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '261cdc020a41e044cfd61b1298bf3349', 'text': 'loT Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a36b38e7840f2576201391a7eabac5b', 'text': 'VAS intey', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2fc533dfd256e95324a9a93517bac539', 'text': 'App serve', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f500655f688a7d8bd46dd5bb338a1b53', 'text': 'Applicatio', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 140, 'parent\_id': '786002fa76029bad3464ec1b2fd1da02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '600f1bc32cbd6254c7db486472b3eb7c', 'text': 'Apart from the expanded threat surface, 5G also presents the security team with an issue of a steep learning curve to identify and mitigate threats faster without impacting the latency or user experience.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 141, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7633a4b928f2e801ac4f31910feb98e4', 'text': 'Although 3GPP provides security enhancements around the user and privacy, it recommends a shared security model, where apart from the inherent 3GPP- specified mandatory requirements on the 5G network components, entities deploying 5G should also ensure that they have a trusted environment to deploy 5G networks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 141, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dd2895b89e82babe9c13482609a9f2bd', 'text': 'Being cloud native and completely software driven, 5G uses open source technologies. Although this is critical for scalability and allowing cloud deployment integrations, vulnerabilities from multiple open source applications could be exploited by attackers. To reduce the attack surface, you will also need to verify the 5G vendor-specific secure development process to ensure hardened software and hardware.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 141, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '87cc4db23b77350b16634fb1046c6672', 'text': 'Chapters 4–9 in Part II, “Securing 5G Architectures, Deployment Modes, and Use Cases,” will take you through the threat model/threat surfaces on end-to- end components of the 5G architecture, including the threats shown in Figure 3-21, and threats on various deployment models, and then explain methods to mitigate them using vendor-agnostic security controls using principles of zero trust.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 141, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd5d2122d162eb4c001e6e9024842ae3c', 'text': 'Acronyms Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 141, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '535f07f98a4ddc313ab2db47e5e7b534', 'text': 'The following table expands the key acronyms used in this chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 141, 'parent\_id': 'd5d2122d162eb4c001e6e9024842ae3c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '7ddf1f633472737c69ea5cab1e1e9094', 'text': 'Acronym Expansion 5GC 5G Core network AES Advanced Encryption Standard AKA Authentication and Key Agreement AMF Access and Mobility Management Function ARPF Authentication Credential Repository and Processing Function AUSF Authentication Server Function CloT Cellular Internet of Things CU Central Unit DN Data network DU Distributed Unit FN-RG Fixed network RG ¢NB NR Node B GUTI Globally unique temporary UE identity IPUPS Inter-PLMN UP Security IPX IP Exchange Service N3IWF Non-3GPP Access Inter-Working Function N5CW Non-5G-capable over WLAN N5GC Non-5G-capable NAI Network access identifier NAS Non-Access Stratum NF Network Function', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Acronym</th><th>Expansion</th></tr></thead><tbody><tr><td>5GC</td><td>5G Core network</td></tr><tr><td>AES</td><td>Advanced Encryption Standard</td></tr><tr><td>AKA</td><td>Authentication and Key Agreement</td></tr><tr><td>AMF</td><td>Access and Mobility Management Function</td></tr><tr><td>ARPF</td><td>Authentication Credential Repository and Processing Function</td></tr><tr><td>AUSF</td><td>Authentication Server Function</td></tr><tr><td>CloT</td><td>Cellular Internet of Things</td></tr><tr><td>CU</td><td>Central Unit</td></tr><tr><td>DN</td><td>Data network</td></tr><tr><td>DU</td><td>Distributed Unit</td></tr><tr><td>FN-RG</td><td>Fixed network RG</td></tr><tr><td>¢NB</td><td>NR Node B</td></tr><tr><td>GUTI</td><td>Globally unique temporary UE identity</td></tr><tr><td>IPUPS</td><td>Inter-PLMN UP Security</td></tr><tr><td>IPX</td><td>IP Exchange Service</td></tr><tr><td>N3IWF</td><td>Non-3GPP Access Inter-Working Function</td></tr><tr><td>N5CW</td><td>Non-5G-capable over WLAN</td></tr><tr><td>N5GC</td><td>Non-5G-capable</td></tr><tr><td>NAI</td><td>Network access identifier</td></tr><tr><td>NAS</td><td>Non-Access Stratum</td></tr><tr><td>NF</td><td>Network Function</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 142, 'parent\_id': 'd5d2122d162eb4c001e6e9024842ae3c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '5757ff44b5cd34eda37ac0db7e154e40', 'text': 'NG Next-Generation ng-eNB Next-Generation Evolved Node-B NG-RAN 5G Radio Access Network NR New Radio QoS Quality of service RES Response SCG Secondary cell Group Scp Service communication proxy SEAF Security Anchor Function SEPP Security Edge Protection Proxy SIDF Subscription Identifier De-concealing Function SMC Security Mode Command SMF Session Management Function SUCl Subscription Concealed Identifier SUPI Subscription Permanent Identifier TLS Transport Layer Security', 'metadata': {'text\_as\_html': '<table><thead><tr><th>NG</th><th>Next-Generation</th></tr></thead><tbody><tr><td>ng-eNB</td><td>Next-Generation Evolved Node-B</td></tr><tr><td>NG-RAN</td><td>5G Radio Access Network</td></tr><tr><td>NR</td><td>New Radio</td></tr><tr><td>QoS</td><td>Quality of service</td></tr><tr><td>RES</td><td>Response</td></tr><tr><td>SCG</td><td>Secondary cell Group</td></tr><tr><td>Scp</td><td>Service communication proxy</td></tr><tr><td>SEAF</td><td>Security Anchor Function</td></tr><tr><td>SEPP</td><td>Security Edge Protection Proxy</td></tr><tr><td>SIDF</td><td>Subscription Identifier De-concealing Function</td></tr><tr><td>SMC</td><td>Security Mode Command</td></tr><tr><td>SMF</td><td>Session Management Function</td></tr><tr><td>SUCl</td><td>Subscription Concealed Identifier</td></tr><tr><td>SUPI</td><td>Subscription Permanent Identifier</td></tr><tr><td>TLS</td><td>Transport Layer Security</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 143, 'parent\_id': 'd5d2122d162eb4c001e6e9024842ae3c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'f47d19f4ddd8bbf1e4af9c63539078f3', 'text': 'TWAP Trusted WLAN access point TWIF Trusted WLAN Interworking Function UDM Unified Data Management UDR Unified data repository UE User equipment up User plane UPF User Plane Function DoS Denial of service DDoS Distributed denial of service V2X Vehicle-to-everything MEC Multi-access edge compute SBA Service-based architecture', 'metadata': {'text\_as\_html': '<table><thead><tr><th>TWAP</th><th>Trusted WLAN access point</th></tr></thead><tbody><tr><td>TWIF</td><td>Trusted WLAN Interworking Function</td></tr><tr><td>UDM</td><td>Unified Data Management</td></tr><tr><td>UDR</td><td>Unified data repository</td></tr><tr><td>UE</td><td>User equipment</td></tr><tr><td>upP</td><td>User plane</td></tr><tr><td>UPF</td><td>User Plane Function</td></tr><tr><td>DoS</td><td>Denial of service</td></tr><tr><td>DDoS</td><td>Distributed denial of service</td></tr><tr><td>V2X</td><td>Vehicle-to-everything</td></tr><tr><td>MEC</td><td>Multi-access edge compute</td></tr><tr><td>SBA</td><td>Service-based architecture</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 144, 'parent\_id': 'd5d2122d162eb4c001e6e9024842ae3c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6c4fcd6a8e9b3799420fea8d8da238f2', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 144, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1732b205c78bbcb85e7e40ad7c1ea3e6', 'text': 'Pramod Nair, “Securing Your 5G Infrastructure to the Edge and Beyond,” Cisco Public, April 1, 2021', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 144, 'parent\_id': '6c4fcd6a8e9b3799420fea8d8da238f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '98375113fca89ec3bd39568ba7324c4a', 'text': 'Pramod Nair, “Securing 5G and Evolving Architectures,” Cisco Knowledge Networks, Cisco Public, September 17, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 144, 'parent\_id': '6c4fcd6a8e9b3799420fea8d8da238f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ab7d2eebcc5d1eeea3440d9f15e54da8', 'text': 'Cisco Systems, “Reimagining the End-to-End Mobile Network in 5G Era,” Cisco Public, 2019', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 144, 'parent\_id': '6c4fcd6a8e9b3799420fea8d8da238f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5e9401a97f33ac8c6f24adab594bfc52', 'text': 'https://www.3gpp.org/', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 144, 'parent\_id': '6c4fcd6a8e9b3799420fea8d8da238f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ba069d7cc759263408785bff34a5e2d3', 'text': '3GPP TS 23.501, “System Architecture for the 5G System; Stage 2” 3GPP TS 33.501, “Security Architecture and Procedures for 5G System”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 144, 'parent\_id': '6c4fcd6a8e9b3799420fea8d8da238f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d4e013314d74ce08ab993533d8d7116', 'text': '3GPP TS 23.501, “System Architecture for the 5G System; Stage 2”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 144, 'parent\_id': '6c4fcd6a8e9b3799420fea8d8da238f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e06640bf20b7a08a8639c29b5570593', 'text': '3GPP TS 33.501, “Security Architecture and Procedures for 5G System”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 144, 'parent\_id': '6c4fcd6a8e9b3799420fea8d8da238f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '87d05de58cfea0ae6fc4c6d555fb23d6', 'text': '3GPP TS 33.402, “3GPP System Architecture Evolution (SAE): Security aspects of non-3GPP accesses”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 144, 'parent\_id': '6c4fcd6a8e9b3799420fea8d8da238f2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f67742e4069dc59bd1905796ef91cd7f', 'text': 'Part II: Securing 5G Architectures, Deployment Modes, and Use Cases”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 145, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '481f3317623f4ea5b1490656c9e333a8', 'text': 'Chapter 4. Securing RAN and Transport Deployments in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '132c0ec4ee399b13dc0f3aed702aed04', 'text': 'After reading this chapter, you should have a better understanding of the following topics:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3be119f5fa88d87efd181f7ace8e63ff', 'text': '• 5G RAN and Transport Threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f42e4bec2a81d2c104a4ce1edfa8e9ad', 'text': '• Securing 5G RAN and Transport', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dbe8a261a021a821421fc86d07d78e8b', 'text': '• Real Scenario Case Study: Examples of Threat Surfaces and Threat Mitigation Techniques', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fe808ea525fcd00305b0366d7a2c6c26', 'text': 'The previous chapter discussed how device-based threats have an impact on a 5G network and different ways of mitigating the threats. This chapter is aimed primarily at the 5G radio access network (RAN) threat surfaces and mitigation techniques for the service provider network. This chapter will be of particular interest to the following teams from service providers and vendors:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1aebbfea1a23320de8fad43aefc9db0b', 'text': '• Mobile infrastructure strategy', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1a21bfc72230bfff4be80dabc26646af', 'text': '• Security strategy', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '43d1f3107884d8d02f33b3fe3f6662e9', 'text': '• Radio planning and optimization', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '88b81b3a0be19687314e8974275c465a', 'text': '• Transmission and the packet core team', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3434e45506cb7332c742720f3471a8fc', 'text': '• Security architects and design teams responsible for securing the mobile infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ab19c08eebe19eac45c11dd806f99ebd', 'text': '• Cybersecurity vendor teams responsible for securing RAN and the transport layer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9ae5b67e1f0cbc7e074e034a55007a0e', 'text': '• Enterprise teams responsible for securing private 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c65f86d913646cbc24d2fa483e5010d6', 'text': 'Along with major technological change meeting the scale requirements for the massive Internet of Things (IoT) and the ultra-low-latency requirements for real-time applications, the new network infrastructure for 5G must simultaneously satisfy increasing demands for bandwidth, high scalability, and the ultra-low-latency needs of new applications and services in an efficient, automated, and programmable manner.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 146, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9b780cccb1e78558655a179a956be29a', 'text': 'In enabling these new use cases, 5G uses technologies such as software-defined networking (SDN), New Radio (NR), virtualization such as Cloud-Native Functions (CNF), Control and User Plane Separation (CUPS), and network slicing. These developments will have significant impacts on the underlying network. For example, depending on the spectrum being used by the service provider, the footprint and the density of the network will need to expand significantly. Hosting new ultra-reliable low-latency communication (URLLC) and massive machine-type communication (mMTC) applications efficiently will require bringing the applications closer to the edge of the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 147, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f07aae52c18015f5f871a8148a4ba2bd', 'text': 'Other key attributes of the 5G transport infrastructure will be to easily carve out and reuse capacity, compute, and resiliency as well as to guarantee latency by supporting network slicing. Service providers will have to manage the network using a completely new approach in order to enable the rapid provisioning and service automation required. In addition to the service provider network–enhancing requirements, the network design needs to cater to the different classes of services, such as fixed line and broadband customers, as well as support the different customer types (consumer, small-to-medium business, and enterprise).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 147, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cb7bf069a02fc097ef4d004ac68d5429', 'text': 'The disaggregation and distribution of the 5G RAN using Distributed Unit (DU) and Centralized Unit (CU) functions allow for openness and the consideration of flexible deployment options. This open and flexible architecture also brings in new threats that require evaluating security options.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 147, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0869ba902dc151040987b51045dee21a', 'text': 'Although there are several security enhancements in 5G as compared to 4G technology, this chapter considers the pragmatic deployments in 5G where the implementation of the 5G network elements and 5G network functions are not always in trusted environments. Apart from the non-trusted 5G network deployment considerations, there have not been enough validations of live 5G networks to ascertain the robustness of the 5G AKA protocol.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 147, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7db2c50b598a9ccd06e4fe1528e36614', 'text': 'The new use cases in 5G also require features such as network slicing, multi- access edge computing (MEC), integration with SDN, and orchestration and automation layers. This necessitates strict granular access control policies to be applied to these layers as well as the need to secure the communication between the 5G network elements and the components enabling the features.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 147, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd15d8aa0d45cef2ff1a88d495b269c25', 'text': 'Service providers deploy different models of transport network. Many service providers follow the model where they own their transport network as well share or lease parts of the transport infrastructure, and security has to be', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 147, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8189767e70768fb7f452eb2fe6c40b23', 'text': 'considered to ensure that the data is secured while passing through all the different transport networks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 148, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6681b108efdcf232f8bd94ff93df7655', 'text': 'Government regulators of many countries also request the service providers to encrypt the end-to-end network to better secure the transport and mitigate any occurrences of data exfiltration from the service provider network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 148, 'parent\_id': '481f3317623f4ea5b1490656c9e333a8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd53ac00306768549154952200261370e', 'text': '5G RAN and Transport Threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 148, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd56e404d3f1e9d983ef0710fe797d48e', 'text': 'This section takes you through multiple options of securing the RAN and the transport and evolving the security posture from 4G toward 5G. It also covers the evolution of the security architecture by looking at security controls (for example, the security gateway evolving from 4G to 5G).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 148, 'parent\_id': 'd53ac00306768549154952200261370e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '975b1df7e4c3a740115d25b79f0d3804', 'text': 'Figure 4-1 provides a high-level view of the threat surfaces in the air interface, RAN, and the transport layer for 5G deployments. The vulnerabilities are explained in more detail in this section.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 148, 'parent\_id': 'd53ac00306768549154952200261370e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'bd35e4a22b616ecd993341e8864bee5c', 'text': '\* Rogue nodes \* Insecure S1, X2 \* Insecure Xx, Xn —» - \* Insecure ZTP/ ZTP / Orchestration / provisioning server i \* Updates with Automation FE malicious codes ( A)) \* Unauthorized user at the orchestration and ) (=) =) automation layer . / ~ e \\ < AT | y = N ~ [ ] [\\ < = s / - Far edge DDoS attacks MEC Centralized 5GC Air interface jamming MitM attacks MitM attack Insecure Sx DosS attacks by force reject messages Insecure N6 Bidding attacks « e e e = UE sniffing and eavesdropping CP/ UP sniffing API vulnerabilities Insecure HW 0S vulnerabilities e ® o \* s o s = e Unauthorized user', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 148, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '8b9d1eb9e00c3754d94dbda321fa62e1', 'text': '=', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 148, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5c358f5c0b7a3eeffa40b98b760a60c2', 'text': 'e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 148, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '07f95cdab6e5cd348aa79e77a94e34fe', 'text': 'e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 148, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ffcea30c1a18dca6a00ccbf246192bc6', 'text': 'e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 148, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '7e066e0c8ae29abc9d70e49eca412834', 'text': '«', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 148, 'parent\_id': 'ffcea30c1a18dca6a00ccbf246192bc6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f44f0a6b466610590848f0bd0d44d4c6', 'text': 'Figure 4-1 RAN and Transport Threats in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 148, 'parent\_id': 'ffcea30c1a18dca6a00ccbf246192bc6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6eb64d00b128dac7601b0c19c73037c5', 'text': 'Vulnerabilities in Air Interface', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 149, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9ae36d97af3e6e743bf867f655e0c075', 'text': 'Although there have been security enhancements in the uplink and downlink air interface communications between the user equipment (UE) and the RAN/packet core in the evolution from 4G to 5G, there are still some unprotected messages in the uplink and downlink. Examples of such messages are Radio Resource Control (RRC) UECapabilityInformation in the uplink and RRC UECapabilityEnquiry and REJECT in RRC/NAS (Non-Access-Stratum) in the downlink. These aforementioned messages being sent unprotected before the Access Stratum (AS) security activation is purely a design choice to enhance the service or connectivity for the user (for example, to provide early optimization for better service connectivity).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 149, 'parent\_id': '6eb64d00b128dac7601b0c19c73037c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1ad3773377c70e63844549379e81689a', 'text': 'An example of such an early optimization would be the gNB sending the UECapabilityEnquiry toward the UE in the RRC message and the UE replying with the UECapabilityInformation, indicating the UE capability. This unprotected message could be exploited by an attacker by using a rogue or fake base station to set up a man-in-the-middle (MitM) attack. Let’s discuss how this could be exploited by an attacker.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 149, 'parent\_id': '6eb64d00b128dac7601b0c19c73037c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '29669aa570e6d4e8b76fbbaa29ef2d70', 'text': 'One of the ways rogue/fake base stations can be set up is by using a Linux box with open-source thin layer of packet core software and radio node software with mod/demod (modulator and demodulator) connected to a power amplifier. Depending on the attack planned by the attacker, an omnidirectional antenna with gain varying from 3 to 6 dBi or a directional antenna with gain around 16 to 18 dBi (depending on the beamwidth of the antenna—the lower the beamwidth, the higher the gain) could be used. For example, if the target is a group of people meeting in a room, a directional antenna would make more impact. However, in a setting such as a crowded area, where the target is not seated and is quite mobile, an omnidirectional antenna provides better results.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 149, 'parent\_id': '6eb64d00b128dac7601b0c19c73037c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b278f44e37b1d7975d4e9467a0f36ae6', 'text': 'The next step is to ensure that the UE is force-camped on to the rogue base station. The procedure of UEs camping on to a base station would depend on whether the phone has just been switched on or whether it’s in a cell selection, cell reselection, or handover procedure. The procedures for cell selection and reselection for 5G are specified in 3GPP TS 38.133.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 149, 'parent\_id': '6eb64d00b128dac7601b0c19c73037c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1587cbc532e28f364548651ce124445e', 'text': 'In 5G, Srxlev indicates the signal strength and Squal indicates the quality of the signal. When camped on a cell, the UE continuously performs measurements to search for a better cell, based on the cell reselection criteria. Depending on the cell reselection criteria, the UE would perform the cell reselection to the same', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 149, 'parent\_id': '6eb64d00b128dac7601b0c19c73037c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1e614bbf51610b8a99e2dffe3460c8e5', 'text': 'radio access technology (RAT) or a different RAT (inter-RAT) as part of the idle mode procedure. Depending on the handover parameters and hysteresis criteria, the UE would perform the handover to the same RAT or a different RAT, specifically 4G (Inter-RAT), as part of the active mode handover procedure. By using the appropriate parameters, the rogue/fake base station can allow MitM attacks to take place by sniffing the air interface for UECapabilityInformation and capturing it. Once captured, the message could be modified to lower the capability level and then forwarded to the real gNB, causing the UE to operate only with restricted or limited radio capability.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 150, 'parent\_id': '6eb64d00b128dac7601b0c19c73037c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6a7e3fcda776f08e4df8a4cb5bcd9d49', 'text': 'A malicious actor might also manipulate the unprotected REJECT messages sent from the network to the UE, which is used to optimize the availability of the system to the connected UE (even in the RRC\_INACTIVE state). The REJECT messages could take the UE out of service. This message could be exploited by the attacker to force UE/5G endpoints from the 5G network to the EPC network. Once the UE is forced to the EPC network, the vulnerabilities existing in the EPC network could be used to exploit the UE and 5G endpoints, such as international mobile subscriber identity (IMSI) spoofing and MitM attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 150, 'parent\_id': '6eb64d00b128dac7601b0c19c73037c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '418eadb6fdd73eef4f224b59d5c4467e', 'text': 'A malicious actor might manipulate the RRCResumeRequest message, where the ResumeCause field is unprotected and hence open to MitM attacks, and the field attribute can be changed. An example is where the attribute value “emergency” can be changed to “ran update.” This change in attribute can cause a big difference in the user service requested by the UE and the service delivered to it. Whereas the user had requested emergency service, the RAN receives the message with ran update and sends the UE to INACTIVE. These kinds of attacks can be aimed at high-value targets or at use cases for critical services.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 150, 'parent\_id': '6eb64d00b128dac7601b0c19c73037c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fd263936e223a90aa7db17b041812b22', 'text': 'A malicious actor might manipulate the weakness in the RRCResumeRequest procedure. When the RRCResumeRequest procedure is initiated by the UE and the gNB is busy, it sends an RRCReject with a wait timer; once the wait timer expires, the UE tries to establish a connection again using the same ResumeMAC-I with the same I-RNTI and Krrcint key, which is the exact same one as the initial request. The attacker can exploit this vulnerability in the air interface and perform MitM attacks such as spoofing the RRCResumeRequest and validating it before the wait timer expiry. This will cause the RRCResume procedure from the original UE to fail, thus causing a denial-of-service (DoS) attack on the UE.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 150, 'parent\_id': '6eb64d00b128dac7601b0c19c73037c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cbbdf36d096f5b53e7d0fb7239543355', 'text': 'Apart from the rogue/fake base station attacks, the threat vector could be from a high-powered device trying to jam a part of the spectrum being used for 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 151, 'parent\_id': '6eb64d00b128dac7601b0c19c73037c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0391c5a03e965d650c3cbea787f3182b', 'text': 'Figure 4-2 illustrates an example of air interface jamming.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 151, 'parent\_id': '6eb64d00b128dac7601b0c19c73037c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'fc68c3ad220eea37950ef58a70039eb9', 'text': '- o ¢ - — - (E———— (%:)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 151, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e060fd3ea8bf32841d2c94cc94689a5e', 'text': 'Figure 4-2 Air Interface Jamming', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 151, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '94e01e4ea488c2ae27b9ade555bf901f', 'text': 'What the jammer actually does is to increase the noise to such high levels that the receiver cannot decode the electromagnetic field (EMF) / radio frequency (RF) signal in the air interface. In certain countries, it is illegal to use jammers for the sole purpose of causing interference with wireless communications. However, sometimes it is made available to cater for use cases such as jamming in military and defense systems for the purpose of electronic countermeasures, such as to deceive radar and other detection systems. This could also be deployed in concert halls to disrupt cellular and Wi-Fi services to prevent distractions from cell phones ringing in the audience. Even though jammers are illegal to obtain, attackers will not find it difficult to make one because the required electronic components are easily found on the open market.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 151, 'parent\_id': 'e060fd3ea8bf32841d2c94cc94689a5e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '992be9329f6e32d94d80d08fa88ec649', 'text': 'Jammers have also become sophisticated and can fine-tune themselves to the frequencies being used by first using a wideband method called sweeping and combing. In this process, the key carriers being used in a cluster or in a specific area are identified by first sweeping the entire spectrum with a high sweep', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 151, 'parent\_id': 'e060fd3ea8bf32841d2c94cc94689a5e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9496b1c9c20126361ce4dbf68bd59993', 'text': 'speed, such as 2–3 GHz per second, and comb-jamming on fixed frequency signals such as 450 MHz. The jammer can also intelligently prioritize the frequency bands it wants to scan based on the data points of user signals found in previous scans. Once the specific frequency band or group of bands in a specific area is identified, the jammer can then choose to pump high-power RF waves in those selected frequency bands, thereby causing very high noise/interference in the area. This leads to the receivers such as legitimate UE unable to establish reliable communication with the service provider base stations in the area, thereby causing a DoS to the receivers (UE) in that particular area.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 152, 'parent\_id': 'e060fd3ea8bf32841d2c94cc94689a5e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9b0939665628ad444753971e65e299b7', 'text': 'Vulnerabilities in the Transport Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 152, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2db6e849e084f4e1e8179d75d7e6f441', 'text': 'Along with major technological change to the mobile core and radio access network (RAN), operators will also need to evolve their transport networks to deliver a satisfying mobile broadband experience in a cost-effective manner, while simultaneously meeting the scale requirements for the massive IoT and the ultra-low-latency requirements for real-time applications. 5G brings in high densification of the network, which requires higher transport access capacity and rich programmable features.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 152, 'parent\_id': '9b0939665628ad444753971e65e299b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0d2c710c0ea4c770e31c4ef5ea512487', 'text': 'To understand the vulnerabilities in the 5G transport network in pragmatic deployments, let’s look at the deployment type being implemented as well as the lack of adequate planning done by a majority of the service providers, which consists of an overlay design including existing 4G eNBs, 5G NSA, and 5G SA gNBs. The new transport design will include terminations in the edge to enable 5G URLLC use cases. Figure 4-3 illustrates an example of the existing 4G-only transport design, which is less dense compared to the transport deployment, which includes 4G and 5G nodes.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 152, 'parent\_id': '9b0939665628ad444753971e65e299b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '200ffe9946de8af52a2118f39cfa6ad3', 'text': '() eNB (<A)) Carrier Ethernet NW (a) ( A) eNB > eNB Service Provider BNG / 4G Transport Access & EPC / Content Delivery (a)a) Backhaul NW ()(A) eNB eNB () Carrier Ethernet NW (3) eNB eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 153, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1047efea81c16b09b4a90b60d61292b5', 'text': 'Figure 4-3 Example of 4G Transport Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 153, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4419e0ebbb98a4dc82ba2749100a20f4', 'text': '5G evolution introduces new capabilities, such as New Radio (NR), a strong reliance on virtualized functions, network slicing, and Control and User Plane Separation (CUPS). These developments, in turn, will have significant impacts on the underlying network. For example, as shown in Figure 4-3, to boost capacity, the footprint of the network will need to expand significantly. To host new URLLC and mMTC applications efficiently, the network will need to be able to integrate regional data centers and distributed compute seamlessly— closer to the endpoints in the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 153, 'parent\_id': '1047efea81c16b09b4a90b60d61292b5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '82d7f01cc354b9b74f84e56f7d33c49a', 'text': 'These edge deployments, consisting of decomposed and distributed 5G CNFs catering for URLLC use cases, coupled with network slicing, require tight time synchronization to support enhanced features such as Coordinated Multipoint (CoMP), which is important in pico cells and small cells aimed at enterprise and industrial IoT (IIoT) deployments. Following the 1588v2-based specifications for synchronization for the transport elements of the network is required. For the frequency sync, 5G Synchronous Ethernet (5G SyncE) and G.8262.1-enhanced Ethernet equipment slave clock (eEEC) requirements have been specified for 5G networks, which have extremely strict demands on frequency drift. This synchronization can be provided by using Global Navigation Satellite System (GNSS) and by delivering sync using transport systems. These GNSS systems are vulnerable because they could be jammed by individuals or malicious entities using channel or spectrum jammers. Any', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 153, 'parent\_id': '1047efea81c16b09b4a90b60d61292b5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '805abbf31384c3459b886209a2102783', 'text': 'attack on synchronization can impact the network performance and, in many cases, cause a DoS to the impacted node or clusters of nodes.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 154, 'parent\_id': '1047efea81c16b09b4a90b60d61292b5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f20055135f56ad58371f4264b5283313', 'text': '5G deployments will be quite dense compared to the 4G deployment, as illustrated in Figure 4-4 (refer to Figure 4-3 for a comparison).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 154, 'parent\_id': '1047efea81c16b09b4a90b60d61292b5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'bc0ea25ab19e9c5d9a22589ad5f5e055', 'text': '(V) (a) A) ( A) gNB gNB Dense Carrier Ethernet NW to ( ) cater for new 5G use cases ) (x) () eNB gNB(( ) (y) (y) eNB W (x) Service Provider 5G / BNG / EPC ((A)) / Content Delivery gNB (e gNB ((A>) ”A) gNB oNB eNB (y) (3) eNB () ( A) eNB gNB 5G & 4G Transport Access & Backhaul NW', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 154, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '989bf063f16cd6bd3548a3b8f7c7ce3d', 'text': 'Figure 4-4 Service Provider Transport Network Evolution Toward 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 154, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '49a48f9542347dd0c9d821c65fd409ed', 'text': 'Figure 4-5 illustrates an example of a rogue transport in the 5G network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 154, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'beaab12cc1519a1c752386df46a874c1', 'text': 'Rogue Router (a) ( A) ((A)) gNB gNB Dense Carrier Ethernet (y) NW to cater for new 5G use cases gNB () ((A>) ong eNB A ( A) eNB eNB (y) Service Provider 5G / (<A)) () BNG / EPC / Content Delivery gNB () X gNB gNB eNB eNB (x) eNB <(A)) ((A)) eNB gNB 5G & 4G Transport Access & Backhaul NW', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 155, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2e59e6e0d02388e1dc23d3518fdce68c', 'text': 'Figure 4-5 Rogue Transport Element in Transport Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 155, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b401da3f3f50a36c1b81d70b48c146d7', 'text': 'This highly dense deployment in 5G introduces another key threat surface related to the intentional or unintentional deployment of rogue access and aggregation transport devices, as illustrated in Figure 4-5.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 155, 'parent\_id': '2e59e6e0d02388e1dc23d3518fdce68c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f5a4b14a9241448ceab3390d93ce958e', 'text': 'very difficult to identity rogue nodes once the deployment is finished. The rogue nodes can be quite easily identified by following best practices such as running basic OS version and vulnerability patching tests before deployment, but usually such deployments will have quite a tight implementation schedule, and many of the security processes might not be observed by the project managers. The key point during these tight deployment schedules is for the project manager to ensure that the tight timelines are being followed, which pushes security process adherence to be last on the priority list (if existent at all). This is the reality in a majority of network deployments, if not all of them. Once the implementation is completed and acceptance testing (AT) is performed, it will be extremely difficult to identify the rogue nodes if they are intentionally deployed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 155, 'parent\_id': '2e59e6e0d02388e1dc23d3518fdce68c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5c6567e21d9891d63dc5d6294f32207b', 'text': 'Other key attributes of the 5G transport infrastructure will be to easily carve out and reuse capacity, compute, and resiliency and to guarantee latency by supporting network slicing. Operators will have to manage the network using a completely new approach in order to enable the rapid provisioning and service automation required. In addition to the pure mobility requirements, operators must also consider how their network caters to the different classes of services they deliver, such as fixed-line and broadband customers, as well as supporting the different customer types (consumer, small-to-medium business, and enterprise). The new network infrastructure must simultaneously satisfy exploding bandwidth demands, massive logical scale, and the incredibly low- latency needs of new applications and services in an efficient, automated, programmable manner.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 156, 'parent\_id': '2e59e6e0d02388e1dc23d3518fdce68c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b2c5b9f864014392de63fb403f92c868', 'text': 'Programmability, while being a critical enabler for the 5G network slicing implementation methods, can also be one of the most vulnerable network elements in the 5G architecture, depending on the level of built-in hardware and software security features of the transport pre-aggregation and aggregation routers and the vulnerabilities within the API implementation, such as the Top 10 OWASP (Open Web Application Security Project) threats. If the virtual instances are built with weak security, such as improperly patched software, or upgraded with malicious code within the upgrade image, it will lead to the entire network being taken into control by the attackers. This is one of the most discussed points by any of the service providers planning to enhance their existing transport infrastructure to cater for 5G or deploying a new transport infrastructure to launch a 5G network. Familiar challenges include physical security, management plane security, control plane security, and potentially exploitable bugs on routing devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 156, 'parent\_id': '2e59e6e0d02388e1dc23d3518fdce68c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d2eeee0d3c16f78126de27d6d0c77ba', 'text': 'As shown Figure 4-6, the programmable transport elements have options of deploying virtualized application instances within the transport device itself to enable URLLC use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 156, 'parent\_id': '2e59e6e0d02388e1dc23d3518fdce68c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c3245100a8cd0c3bc102cfb2719bc5ac', 'text': "- Attacker Malicious code within patches API vulnerabilities Virtual Virtual instances instances = iy ' /m. | lllﬂ ia° K > CEEe Insecure MEC Insecure fild programmable programmable Centralized packet core pre-aggregation aggregation/ router backhaul router", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 157, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '60d98cebc0d446d6689b960cb9313461', 'text': 'Figure 4-6 Attack Scenario in the Transport Network Due to Insecure API', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 157, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '25501f30c08fb396f887e5e93473069f', 'text': 'Another threat vector for transport network devices is from attackers using the Plug and Play (PnP) or provisioning server to take control of the transport network elements.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 157, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '83842a4331b0b219a5a7dbde11bfe5af', 'text': 'As shown in Figure 4-7, most of the transport routers (front haul, mid haul, and back haul) on the market today use the Zero-Touch/PnP/provisioning server for initial configuration of the transport routers and also to deploy patches and automatically install them.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 157, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '72ee87b83bbcdf1d92c66248d7897969', 'text': 'Internet ((A» Pre-aggregation i gNB router MEC Aggregation/ Centralized backhaul router packet core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 157, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '37bd2940c2af55d37749717efa5ce179', 'text': 'Figure 4-7 Configuration of Transport Routers Using Provisioning Servers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 158, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '86119c991a30cd80800e07255768fed8', 'text': 'As Figure 4-8 illustrates, the attackers can take control of the provisioning server and force-download malicious updates to the transport network elements. Once the malicious code is installed on the transport network elements, the entire 5G network is compromised. The impact of such an attack could be very dangerous, including taking several servers down and causing an outage for an extended period of time.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 158, 'parent\_id': '37bd2940c2af55d37749717efa5ce179', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'abe58967d01f5ebe1a4ae2de33eff0be', 'text': '. Attacker [ %] PnP / provisioning server Malicious codes Internet deployed as rogue & updates &) +——iEss— = > fid Pre-aggregation Aggregation/ (: eg) router backhaul router Centralized packet core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 158, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b509827af83ee22bec22d0dd4b0fc750', 'text': 'Figure 4-8 Attack Scenario in Transport Network Due to Insecure Provisioning Server', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 158, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b9e7f47de250166dcbca3e35bafa1a6d', 'text': 'Rogue/Fake Base Station Vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 158, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fe8368284daae03312dde3a6c7cca6b1', 'text': 'One of the key threat vectors in 5G RAN and the transport layer involves rogue/false base stations and IMSI catchers. This section covers the impact on the network and subscribers due to fake/rogue base stations. The 5G system in particular has already made significant security enhancements to combat false base stations—improvements such as guaranteed GUTI (Global Unique Temporary Identifier) refreshment, SUPI (Subscription Permanent Identifier) concealment, protected redirections, and also security features inherited from', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 158, 'parent\_id': 'b9e7f47de250166dcbca3e35bafa1a6d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ab7567c5b123f2e61d7f11247b2f35f7', 'text': 'earlier generations, such as mutual authentication between the UE and network, integrity protected signaling, and secure algorithm negotiations.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 159, 'parent\_id': 'b9e7f47de250166dcbca3e35bafa1a6d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1531f6a35b4574c0fc0ba600a1bfa8a3', 'text': 'Although there are security enhancements in 5G technology as compared to 4G, there are also threat vectors that are not mitigated by those enhancements. The key threat vectors and risks due to fake/rogue nodes are mainly related to MitM attacks, where the key aim of the attacker is to maliciously perform snooping and gain insight on specific subscribers or groups of subscribers. This method primarily targets network clusters serving 5G devices in critical infrastructure deployments and clusters providing coverage to high-profile industry verticals and embassies. Some of the key threat vectors and risk examples are detailed in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 159, 'parent\_id': 'b9e7f47de250166dcbca3e35bafa1a6d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '352120d9d4e540a985c09eef6c3b47d4', 'text': '• A MitM false base station may perform a linkage attack via Subscription Concealed Identifier (SUCI) replay. That is, it replaces a SUCI in a registration request or in an identity response by a previously captured SUCI and observes whether the UE will be authenticated and receive service.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 159, 'parent\_id': 'b9e7f47de250166dcbca3e35bafa1a6d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6ac6e0356be3d6e0762aeb2669c55dd0', 'text': '• Using a rogue/false base station, an attacker may launch various types of attacks, such as transporting security-protected messages without any modification while dropping, altering, and/or injecting unprotected messages such as the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 159, 'parent\_id': 'b9e7f47de250166dcbca3e35bafa1a6d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '83c33df7243ac961a2e6e8814f5473d7', 'text': '• Pre-authentication traffic', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 159, 'parent\_id': 'b9e7f47de250166dcbca3e35bafa1a6d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f2e34043e06918e270cbd6c417ebddf2', 'text': '• MAC/RLC layer message headers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 159, 'parent\_id': 'b9e7f47de250166dcbca3e35bafa1a6d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bb2b307587ba2e349261fb3408f3fef1', 'text': '• Lower layer control messages such as buffer status reports', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 159, 'parent\_id': 'b9e7f47de250166dcbca3e35bafa1a6d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cbd1b2788d0fec5b5b27651ecc897ddc', 'text': '• A MitM attack could also include replaying messages (that is, the MitM sits between the actual base station and the UE and forwards the messages of the base station to the UE and the messages of the UE to the base station). In this position, the MitM might do nothing for a very long time, making it very difficult to detect. However, on certain occasions, the MitM might inject/alter/drop messages. The basic requirement to defeat MitM attacks is often related to replay protection.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 159, 'parent\_id': 'b9e7f47de250166dcbca3e35bafa1a6d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '39c2d6c35df0d594ffc1f3dcdbb5d183', 'text': '• A MitM false base station might force the UE to camp on to it by passing all the messages between the UE and the real base station. It might then reject or drop service requests, not pass on paging messages from the UE, and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 159, 'parent\_id': 'b9e7f47de250166dcbca3e35bafa1a6d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c09338670baa7639f0af6677377acfac', 'text': '• When UP integrity protection is not used, a MitM false base station might trick the UE into accessing malicious websites or it might even impersonate the UE on the IP layer, which includes the decryption of downlink traffic and performing encryption of faked uplink traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 160, 'parent\_id': 'b9e7f47de250166dcbca3e35bafa1a6d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2ff3a85f627e1b8475c75d7ce40ee06e', 'text': 'Securing 5G RAN and Transport', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 160, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '99fca9a06532abc1d0ebb65b026f0056', 'text': 'Although there are several security enhancements in 5G as compared to 4G technology, this chapter considers the pragmatic deployments in 5G where the implementation of the 5G network elements and 5G network functions are not always in trusted environments. Apart from the non-trusted 5G network deployment considerations, there haven’t been enough validations of live 5G networks to ascertain the robustness of the 5G AKA’ protocol.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 160, 'parent\_id': '2ff3a85f627e1b8475c75d7ce40ee06e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c5b78d9492f693d5551312624c14d928', 'text': 'Securing the Air Interface', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 160, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b2e33daa3acd39f9bc7b2d772e2ddf62', 'text': 'To bring more openness to 5G, the 5G authentication is made access-agnostic, meaning that it should support both 3GPP access (cellular networks) and non- 3GPP access (Wi-Fi and cable) networks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 160, 'parent\_id': 'c5b78d9492f693d5551312624c14d928', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '876a16e7f20213d4dd10df9b9585eea3', 'text': 'To make the connections from both 3GPP and non-3GPP more secure, 5G uses a new unified authentication framework. The initial registration procedure used for 4G, called Primary Authentication in 5G, now also supports a widely used protocol in IT called Extensible Authentication Protocol (EAP) Authentication and Key Agreement (EAP-AKA), which allows different types of credentials such as username and passwords, certificates, and pre-shared keys (PSK). This further extends 5G authentication to devices used in IT, factory, and industry verticals.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 160, 'parent\_id': 'c5b78d9492f693d5551312624c14d928', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bcb997d0faa95b62e6b41b9ff275b943', 'text': 'Apart from the primary authentication, 5G now also supports secondary authentication—a separate authentication and authorization procedure that can be performed by external data networks or the service provider apart from the initial primary authentication performed by your network. EAP is supported for the secondary authentication procedure, which can be executed by the external data network or service provider. The purpose of the primary authentication and key agreement procedures is to enable mutual authentication between the UE and the network and provide keying material that can be used between the UE and the serving network in subsequent security procedures.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 160, 'parent\_id': 'c5b78d9492f693d5551312624c14d928', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ecafbe95dcd9c5cdfee566ce5b1b0933', 'text': 'As an example, your network will perform the initial primary authentication when the UE tries to connect to your network. When the same UE tries to connect to an external network, your 5G network will use EAP to request the external network to perform a secondary authentication with a separate AAA (authentication, authorization and accounting) server owned by the external network. The UE will be permitted connectivity to the external network only after successful secondary authentication.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 161, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cc9684c6cca22e9d0b052335267c7a91', 'text': 'The three authentication methods are as follows.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 161, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2a9663ed81eaaff5814b46b54411ab8', 'text': '• 5G-AKA: 5G-AKA enhances EPS-AKA used in 4G by providing the home network with proof of successful authentication of the UE from the visited network. The proof is sent by the visited network in an Authentication Confirmation message. It provides mutual authentication between the UE and the 5G network. Both 5G-AKA and EAP-AKA’ use the shared key Ki stored in the USIM for the AKA protocol when the UE connects to the cellular network. The authentication procedure includes the UE requesting access by sending its SUPI to the network. In 4G, this was unencrypted, leading to the risk of interception; in 5G, it is encrypted. The 5G network responds to this request by sending an Authentication Vector to the UE. The UE must encrypt this using the shared-key Ki and send it as the response. Because the home network has a copy of the key, it can validate the decrypted response.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 161, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4abaaa2717f903b60a447690c17f2860', 'text': '• EAP-AKA’: EAP-AKA’ is a small revision of the Extensible Authentication Protocol method for the 3G Authentication and Key Agreement (EAP-AKA) method. The change is a new key derivation function that binds the keys derived within the method to the name of the access network. This limits the effects of compromised access network nodes and keys.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 161, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '880339bc1a5d6bd4f259c5d1c41e99fc', 'text': '• EAP-TLS: EAP-TLS is used in 5G when the devices do not support USIM. EAP-TLS uses the TLS public key certificate authentication mechanism within EAP to provide mutual authentication of client to server and server to client. With EAP-TLS, both the client and the server must be assigned a digital certificate signed by a Certificate Authority (CA) that they both trust. When selected as the authentication method, EAP-TLS is performed between the UE and the AUSF. For mutual authentication, both the device and the AUSF can verify each other’s certificate.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 161, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '87a204ddf4bd71276e0f683935f2e2dc', 'text': 'The 5G technology also allows for attributes such as wait timers to be configured to combat some of the attacks from rogue/fake base stations, such as the REJECT attacks mentioned earlier.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 162, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '92339ed4c836eb94cc3951349f287a79', 'text': 'One method of detecting rogue base stations, rogue repeaters, and jammers is by first using key performance indicators (KPIs) of the sectors and cells covering the area to understand the clusters of cells showing high interference or drops due to interference or bad quality signal. Once the 4G or 5G cells or clusters of 4G or 5G cells are identified as being impacted by the interference, a drive test can be carried out in the identified area using drive-test equipment and spectrum analyzers to detect the jamming equipment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 162, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd61aaf2fcd2903cda5590444436954c6', 'text': 'Using Trusted Transport Network Elements', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 162, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e52757e117f6ceda4d7731ffe9757504', 'text': 'Given that most aggregation devices will be placed in untrusted or partially trusted environments, strong emphasis on tamper-proofing is essential. Beyond this concern, 5G enlarges the problem with network data center compute elements, software running on those elements, and new orchestration capabilities that must also be secured.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 162, 'parent\_id': 'd61aaf2fcd2903cda5590444436954c6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3fccb3453dc261ea5770daa3006e6a11', 'text': 'Service providers planning to build the transport infrastructure should ensure that the transport vendor has products designed with security as a foundation, starting from the built-in secure silicon to deliver platform trust, network trust, and application trust. There are vendors in the market today using trustworthy systems for securely storing unique cryptographic keys in hardware and capabilities like secure boot.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 162, 'parent\_id': 'd61aaf2fcd2903cda5590444436954c6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4eea44fd141a9919f583fca654b1b2b9', 'text': 'The foundation of a trusted network is trusted devices, and all trust must begin in hardware by utilizing technologies such as Trust Anchor, which establishes a hardware root of trust for software integrity and strong encryption. This hardware security component provides a unique cryptographic identify of each platform component and should be used as the basis for the advanced secure boot infrastructure by the vendor you select for 5G deployments. Hardware- rooted secure boot infrastructure–based platforms provide significantly stronger protections against compromises of the firmware and operating system than typical firmware-based secure boot infrastructures (such as those used in mainstream x86 platforms). This, coupled with advanced runtime OS protections and control-plane protections, provides the platforms with unique capabilities to establish and maintain trust in exposed environments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 162, 'parent\_id': 'd61aaf2fcd2903cda5590444436954c6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e435ee39ac20ae525caf876a81c06aa6', 'text': 'Apart from the built-in security layers mentioned, additional security services such as strong cryptographic protection for secret data and key material within the router should also be catered for. 5G will be increasingly deployed in insecure remote locations, and this built-in hardware-keyed protection for secret data at rest is required to maintain trust and control of critical network services.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 163, 'parent\_id': 'd61aaf2fcd2903cda5590444436954c6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c118988474534b9342630e7eff6caa82', 'text': 'Secure Deployments and Updates Using Secure ZTP', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 163, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f0a374d8876e95e1da5ae03b92368e22', 'text': 'As explained earlier in the section, “Vulnerabilities in the Transport Network,” 5G use cases and deployment options will bring in higher densification and programmable capabilities to allow seamless integration with SDN.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 163, 'parent\_id': 'c118988474534b9342630e7eff6caa82', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a32f4186ff6706f102764afe0aed0562', 'text': 'In most transport network deployments, service providers receive their purchased routers and usually ferry them to pre-staging facilities as part of the first “truck” rollout. At the prestaging facility, the devices are typically configured manually with the help of technical personnel to place bootstrap configurations on them. These pre-configured boxes are then shipped out to the installation site, often using third-party installers to simply set up and power on the devices that were pre-staged. This constitutes the second “truck” rollout. This might not be the exact workflow for all network operators, but it’s fairly representative of the workflows in use across a majority of them.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 163, 'parent\_id': 'c118988474534b9342630e7eff6caa82', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ef68f3c5dbdf4e2381bb28cb57975dab', 'text': 'The use of competent technical personnel at pre-staging facilities, the multiple truck rollouts, the post-installation rollouts, and corrections in case of errors in the bootstrap configurations all contribute to the consistently rising operational expenses (OPEX) that most large-scale service providers incur. As the number of devices in these deployments continues to grow to meet consumer demands and newer 5G architectures, it is imperative to find techniques to reduce the OPEX as much as possible.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 163, 'parent\_id': 'c118988474534b9342630e7eff6caa82', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5aa2847a7356c14a41190f857e4f4851', 'text': 'Apart from the preceding key points, the mitigation of rogue transport access devices, such as rogue access and aggregation routers, is very critical to the end-to-end security of the 5G network. To allow for optimized OPEX and have secure automation for the deployment and operation of the transport access devices, services providers have to use Zero-Touch Provisioning (ZTP) and Secure ZTP (SZTP) techniques.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 163, 'parent\_id': 'c118988474534b9342630e7eff6caa82', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ff59c3724d409752da69ae2d9157e108', 'text': 'ZTP automates the process of installing or upgrading software images and installing configuration files on transport access devices that are deployed for the first time in the network. It reduces manual tasks such as upgrading and', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 163, 'parent\_id': 'c118988474534b9342630e7eff6caa82', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c5205909c7d983890fa98fbf371c878e', 'text': 'configuring the devices. ZTP is one of the most critical features for 5G transport access network elements, as service providers are looking to automate Day 0 provisioning of routers to help reduce the OPEX associated with technical personnel and staging facilities used today. ZTP is also important for the patch and updates process.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 164, 'parent\_id': 'c118988474534b9342630e7eff6caa82', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '590199208172b94d761c26809dd710d0', 'text': 'SZTP is a bootstrapping strategy that includes updating the boot image, committing an initial configuration, and executing arbitrary scripts to address auxiliary needs to enable devices to securely obtain bootstrapping data with no installer action beyond physical placement and connecting network and power cables. The updated device will subsequently be able to establish secure connections with other systems. For instance, a device might establish NETCONF and/or RESTCONF connections with deployment-specific network management systems. SZTP also enables nontechnical personnel to bring up devices in remote locations without the need for any input from your end.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 164, 'parent\_id': 'c118988474534b9342630e7eff6caa82', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9e7f0b6adbd3a5c16f9f3f38b3da1125', 'text': 'You should follow SZTP, at a minimum, to ensure the secure deployment and secure lifecycle of the transport access network elements.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 164, 'parent\_id': 'c118988474534b9342630e7eff6caa82', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '585b2d7e35d493185a41372bd9447cf3', 'text': 'As shown in Figure 4-9, provisioning servers following SZTP techniques can be used to provision and manage patches and updates to the entire transport access network. When a device that supports ZTP boots up and does not find the startup configuration (during a fresh install on Day 0), the device then enters ZTP mode.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 164, 'parent\_id': 'c118988474534b9342630e7eff6caa82', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ccb23cc6c10d5480e49120d97b0e375b', 'text': 'PnP / provisioning server based on SZTP lechniqu\\es ( \\ o — | | [\*=] | Private / public cloud | & R CU R et identified Rogue Router ((A)) ((A)) gNB gNB ((A)) gNB ) (a) eN oNB|( A (p) (p) eNB ) eNB ((A)) ((A)) W/ gNB (W) gNB gNB eNB eNB ((A» ( ) eNB (<A)) gNB =T', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 165, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '17fd0e9034c71f91b13ece8c64289738', 'text': 'Figure 4-9 Mitigation Example of Rogue Transport Device Scenarios', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 165, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a3383d782e7b00942a6e1b666b0b7120', 'text': 'In ZTP mode, the device locates a Dynamic Host Control Protocol (DHCP) server, bootstraps itself with its interface IP address, gateway, and Domain Name System (DNS) server IP address, and enables Guest Shell. The device then obtains the IP address or URL of the provisioning server depending on the deployment method chosen by the service provider.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 165, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2ee96147ad89c20f5776c1091f72354f', 'text': 'You should deploy the provisioning server using SZTP techniques to enable configuration of only trusted transport access devices, this will mitigate the threat vectors from untrusted transport network devices. To adhere to SZTP procedures, the service provider’s network management system (NMS) would need to authenticate the IDevID certificates (the NMS obtains from the manufacturer the trust anchor certificate for the IDevID certificates during the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 165, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2e7364f339296a1c49451c0d0aee3138', 'text': 'initial enrolment process), and only the genuine devices would be authenticated. This would allow the detection of the rogue transport access device, which can then be removed from the network, or further investigation can be done to understand how it was present in the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 166, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f67f5407aa4dbe87802b2129e6d2ab8', 'text': 'By following the described SZTP process and best practices in the list that follows, you can better secure the transport access network and mitigate the threat vectors, such as the deployment of rogue transport access devices, in the service provider network:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 166, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9a5e67a0186a0413de12343a84fdf9f9', 'text': '• Ensure that the transport infrastructure device has built-in hardening mechanisms such as tamper resistance, tamper detection, tamper response, and tamper evidence to mitigate any hardware tampering of the transport device.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 166, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5314d5e98312b5afa70fe6b2f5be998f', 'text': '• Ensure that the proper enrollment process is followed by the service provider and the device vendor/manufacturer in the pre-deployment stage.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 166, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '08f553bf1903a915e9c0683393093944', 'text': '• Ensure that the device has the pre-configured state and SZTP bootstrapping flag set to “true” to enable SZTP bootstrapping to run when the device powers up for the first time.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 166, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ffe65f4e722cc3ffcf6d4d778dccfef4', 'text': '• The device should have the private key for the TLS client certificate and the private key for decrypting SZTP artifacts securely stored, ideally in a cryptographic processor such as a trusted platform module (TPM).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 166, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ea9ce33bc63fd97b2ec281908b0bbe43', 'text': '• Ensure that the transport device can be validated. This can be achieved by making sure that the SZTP server can validate the certificates provided by the device in the initial request.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 166, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '17c7aa4bcb047dc72d9f258ce2e77d88', 'text': '• Ensure that the SZTP server can be validated to make sure the device is joining the correct network. This can be done by loading the owner certificate onto the device in the factory provisioning process by the device manufacturer, which is then validated against the domain certificate or the ownership voucher during the SZTP server interactions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 166, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b75ae393234a4bc87c3d283090fad94d', 'text': '• Ensure that the boot image is securely booted using the principles of Secure Boot provided in the Unified Extensible Firmware Interface (UEFI) specifications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 166, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a6c95eba296f640fa095bc1a41810e75', 'text': '• Ensure that the user access control to the bootstrapping server and the SZTP server follows strict access control and has very granular access policies applied to it.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 166, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '266a264122cc7c17e908e27b8f1ce07f', 'text': '• Ensure that the pre-configuration scripts, initial configuration scripts, and post-configuration scripts are thoroughly validated by the NMS teams and by the service provider in a lab or a pilot network before being deployed in a production/live network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 167, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '95cb977114ad6f2b582bbeb234843e8e', 'text': '• Ensure that the source of the software update is validated and has a process in place where the software update is first applied to a lab or pilot transport network. Only after thorough investigation of the pre- and post- update behavior should the update be allowed to be deployed in the production or live network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 167, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '42845c29e98d0d359a1e4e2e567101d2', 'text': 'Using Security Gateway (SecGW/SEG) to Secure the RAN and Transport Layer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 167, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b65a1491acd319039e33fdf04aebe672', 'text': 'One of the main concepts introduced in 3GPP 33.210 is the notion of a security domain, which is a network managed by a single administrative authority. Within a security domain, the same level of security and use of security services is typical. Normally, a network run by a single network operator or a single transit operator will constitute one security domain, although an operator may at will divide the network into separate subnetworks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 167, 'parent\_id': '42845c29e98d0d359a1e4e2e567101d2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6147fd733ee5686d33b4d95bfca8d204', 'text': 'The border between the security domains is protected by a security gateway (SecGW or SEG). The SecGWs are responsible for enforcing the security policy of a security domain toward other SecGWs in the destination security domain. The network operator might have more than one SecGW in its network in order to avoid a single point of failure or for performance reasons.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 167, 'parent\_id': '42845c29e98d0d359a1e4e2e567101d2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ef923553d778207d15dd80b27a9302e', 'text': 'Figure 4-10 depicts a network with a 5G gNB and an LTE eNB. The network has traffic passing through the untrusted and insecure transport layer, which is not owned by the operator, and terminates the traffic in the multi-access edge compute (MEC). The traffic from the MEC is also passing through the untrusted network before it gets terminated in the centralized packet core.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 167, 'parent\_id': '42845c29e98d0d359a1e4e2e567101d2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '17eea3824268f313d812cc1383ccf2df', 'text': '- g\\B rE=e » s = MEC Centralized 4G & 5G Packet Core eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 168, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed321b6422c4492b135924e1c30acef7', 'text': 'Figure 4-10 Transport Network Using an Insecure Public Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 168, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b6068e217ffe6b04509e619afe6df7fb', 'text': 'Figure 4-11 shows the deployment of the SecGW to terminate all the IPsec tunnels from the gNB and eNB and also to secure the traffic between the MEC and the centralized packet core. The network collectively uses distributed and centralized security gateways to secure the end-to-end transport of the 4G and 5G infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 168, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5d4b62c9f746e3a3c64e574738adc53c', 'text': '((A)) agNB = i MEC Centralized 4G&56G Packet Core ( A)) « eNB \\—Y—/ Transport secured by IPsec end to end', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 168, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '29a3a1b99cbc1d72d058732a58e5f8f1', 'text': 'Figure 4-11 Securing a Transport Network Using IPsec', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 168, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '590d578445fd68299099c2183e63faab', 'text': 'The primary concerns for any service provider planning the back haul are the security of the data and preventing eavesdropping when the data traverses the insecure transport infrastructure, be it a public network or a partner network. One way to do this is by encrypting the data by deploying encryption and decryption at each site and introducing authentication mechanisms to ensure devices providing encryption and decryption are legitimate.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 168, 'parent\_id': '29a3a1b99cbc1d72d058732a58e5f8f1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8cc3f2f736509cfa86da61fb45cc8003', 'text': 'IPsec is a suite of protocols developed under IETF to provide authentication, integrity, access control, and confidentiality. The fundamental components of IPsec are defined in the RFC 2401 and described in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 169, 'parent\_id': '29a3a1b99cbc1d72d058732a58e5f8f1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58e644069803cd6ed9649e13ffe07153', 'text': '• Security protocols: Authentication Header (AH) and Encapsulation Security Payload (ESP)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 169, 'parent\_id': '29a3a1b99cbc1d72d058732a58e5f8f1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c929b840c4c8c349d0a7389a20b49b8c', 'text': '• Key management: ISAKMP, IKE, and SKEME', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 169, 'parent\_id': '29a3a1b99cbc1d72d058732a58e5f8f1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da9037d46e6dc0c835bc2fb554a40aae', 'text': '• Algorithms: Enabling encryption and authentication', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 169, 'parent\_id': '29a3a1b99cbc1d72d058732a58e5f8f1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '518713afbf37745f47514ac2fd6f3368', 'text': 'The security gateway provides the IPsec functionality. Using a security gateway ensures that the data transferred between the 4G and 5G radio nodes (eNB/gNB) and the packet core (EPC/5GC) and the data transferred using an insecure transport network is encrypted and verified.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 169, 'parent\_id': '29a3a1b99cbc1d72d058732a58e5f8f1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd648f5670708adf6c24bc983a09b820b', 'text': 'Centralized SecGW', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 169, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5c21b38a4f7f5ff734ea8cde9e4537d4', 'text': 'In more centralized environments, where there are fewer geographic sites or there is a requirement for larger-scale clusters of IPsec termination (that is, massive throughput), the centralized SecGWs should be able to create large pools of IPsec capability and be able to statefully inspect the traffic entering and leaving the tunnel. These SecGWs can also be positioned in a geographically dispersed environment if stateful inspection is required, and they should be able to provide resiliency by configuring it as active/standby, active/active, or clustered. as needed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 169, 'parent\_id': 'd648f5670708adf6c24bc983a09b820b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '22831ee32f36f61becacf1e1f32a4a0e', 'text': 'Distributed SecGW', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 169, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fcc110a8c3a06a6a47340736f94359fe', 'text': 'The distributed SecGW provides a fully distributed IPsec termination capability to the very edge of the network. This is requisite for the 5G URLLC use cases and 3GPP LTE-A X2 latency requirements when features such as Coordinated Multipoint (CoMP) are enabled. The inclusion of a distributed SecGW does not negate the requirement for a geographically dispersed/centralized SecGW. The main purpose is to ensure that the UPF can be deployed in distributed MEC layers and the X2/Xn/Xx traffic can be forwarded between 4G and 5G nodes with minimal latency. For many service providers, the plan is to deploy both centralized and distributed SecGWs instead of having to choose between the two modes of SecGW deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 169, 'parent\_id': '22831ee32f36f61becacf1e1f32a4a0e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b97a3cbfe8ad4ddbea549c86c6f15499', 'text': 'Interfaces Secured by SecGW', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 169, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bb8566af452ad51d9d6f9c9aaf2c07a3', 'text': 'Figure 4-12 shows the key interfaces of 5G, which are secured using the centralized/distributed SecGW deployment. The security services that have been identified as being needed are confidentiality, integrity, authentication and anti-replay protection. These will be ensured by standard procedures, based on cryptographic techniques provided by the SecGW. Please note that as per 3GPP specification 33.501, IPsec support is mandatory in 5G gNB. So for the N2 and N3 interfaces, the IPsec tunnel can be initiated by the gNB toward the SecGW without any SecGW deployment at the gNB location. 5G gNB can also terminate the IPsec tunnel from the SecGW without any need for SecGW deployment at the 5G gNB location.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 170, 'parent\_id': 'b97a3cbfe8ad4ddbea549c86c6f15499', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '0666de7ee2967f1e1348d32be5161dbd', 'text': 'N2 N2 N4 o N3 N4 N3 Central DC 5GC o (<A>) 3\\ (UPFUPF N6 5G RAN MEC l ( A))', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 170, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'text': 'Figure 4-12 Securing 5G Interfaces Using a Security Gateway', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 170, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c8d0c593d340d16569c6d1d62df7a676', 'text': 'For the IPsec tunnel between the MEC and central DC 5GC, specifically for interfaces such as N4, a separate SecGW would be required in the MEC and central DC to establish the IPsec tunnel.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 170, 'parent\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b24c2ad1390cb94436169e6046fd858e', 'text': 'In Figure 4-12, the following interfaces are secured by using a SecGW:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 170, 'parent\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6b406cbef2291460c28ac42abe9813b1', 'text': '• The N2 interface, which uses SCTP (NGAP), supports the control plane signaling between 5G RAN and 5G Core covering UE context management and PDU session/resource management procedures. In the figure, N2 is shown as deployed in the central DC 5GC, which most of the service providers are planning to implement, but it can be located at the MEC DC, depending on the deployment option chosen by the service provider. N2 being signaling doesn’t impact the low-latency use cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 170, 'parent\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1242d33e5270187b72bbdb1a807221f9', 'text': 'much (depending on the low-latency requirement of the use case) and is hence normally planned to be deployed in the central DC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 171, 'parent\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0f137479fa9fa469b596bc422dc62185', 'text': '• N3, the interface between 5G RAN and the UPF, carries the user plane data from the UE to the UPF. In Figure 4-12, the UPF is located at the MEC, and hence the N3 is terminated at the MEC layer. N3 uses the GTP (GPRS Tunnelling Protocol) with header extensions for 5G, segment routing (SR), and so on. For the service provider, the location of deployment for the UPF is also dependent on the use cases. For example, for some of the IoT use cases, the UPF is still planned to be deployed in the central DC. The location and the level of security in the deployment location would determine the need for securing the N4 interface using IPsec ESP and IKEv2 certificate-based authentication provided by the SecGW.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 171, 'parent\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '27a665ce1a6be45dd8fdfaacb47fa782', 'text': '• N4, the interface between the User Plane Function (UPF) and the Session Management Function (SMF), uses the Packet Forwarding Control Plane (PFCP) protocol, which was also used in the Sx interface in the 4G CUPS architecture. The location of deployment of the UPF (that is, whether the UPF is co-located with the SMF or is distributed) would determine the need for securing the N4 interface using IPsec ESP and IKEv2 certificate- based authentication provided by the SecGW.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 171, 'parent\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e704105be39907ced8765f99761c8bce', 'text': 'Apart from the preceding interfaces shown in Figure 4-12, other interfaces can be secured by the SecGW, as described in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 171, 'parent\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ee458d3e273e02813755c649a0c728dc', 'text': '• The Xn interface connecting the 5G RAN nodes, consists of Xn-C, carries signaling and Xn-U, and carries user plane data. In addition to IPsec ESP and IKEv2 certificate-based authentication provided by the SecGW, Datagram Transport Layer Security (DTLS) can also be used to provide integrity protection, replay protection, and confidentiality protection. The decision of whether to terminate the Xn interface in the distributed or centralized security gateway is dependent on the network topology of the RAN nodes’ deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 171, 'parent\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '634e4bb5d7ed5d9b4bee5ae7ddd7387b', 'text': '• The Xx interface connecting the 5G RAN nodes with the 4G RAN nodes consists of Xx-C, carries signaling and Xx-U, and carries user plane data. In addition to IPsec ESP and IKEv2 certificate-based authentication provided by the SecGW, DTLS can also be used to provide integrity protection, replay protection and confidentiality protection. The decision of terminating the Xn interface in the distributed or centralized security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 171, 'parent\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e84cd10c569ee74932cbcd3cf813ad8f', 'text': 'gateway is dependent on network topology of the RAN nodes deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 172, 'parent\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd246d99707279521e800ec7a47d694ad', 'text': '• The F1 interface connecting the gNB-CU to the gNB-DU consists of F1-C, carries control plane data and F1-U, and carries user plane data. The IPsec ESP & IKEv2 certificate-based authentication support on the gNB-DU and gNB-CU is mandatory, but the deployment of cryptographic solutions such as SecGW is purely the decision of the service provider. Due to the dynamic nature of the gNB-DU, it is recommended to have the SecGW at the gNB-CU location which can terminate the IPsec from multiple gNB- DUs. In addition to IPsec ESP and IKEv2 certificate-based authentication provided by the SecGW, DTLS can also be used to provide integrity protection, replay protection, and confidentiality protection as documented in RFC 6083.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 172, 'parent\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aebd4daab5da1456b1649c90049c5b91', 'text': '• The E1 interface connecting the gNB-CU-CP to the gNB-CU-UP is used for the transport of the signaling data. The IPsec ESP & IKEv2 certificate- based authentication support on the gNB-DU and gNB-CU is mandatory, but the deployment of cryptographic solutions such as SecGW is purely the decision of the service provider. In addition to IPsec ESP and IKEv2 certificate-based authentication provided by the SecGW, DTLS can also be used to provide integrity protection, replay protection, and confidentiality protection, as documented in RFC 6083. Per the service provider, the gNB-CU-CP and gNB-CU-UP are co-located, sometimes even in the same rack, and hence might not require the SecGW to be deployed. This, of course, would depend on the deployment option chosen by the service provider, the location of the edge/far-edge DC, and who owns the edge/far-edge DC (that is, whether it is a shared infrastructure or deployed in a public or private cloud infrastructure).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 172, 'parent\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '44131f5bd163b369fbba2e464e4f745c', 'text': 'The deployment options of the SecGW and the interfaces being secured will be explained in more detail throughout the chapters in this part of the book.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 172, 'parent\_id': 'aba7b9ce0b26ec3ba3ed0b947c36de03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5dbd25cbf7554e1be5354758518f2991', 'text': 'Set of Features Required by the Security Gateway in 5G Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 172, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '406a8067ea8bb148176696adf4588c34', 'text': 'For service provider networks, the IPsec security protocol should always be ESP; it is further mandated that integrity protection/message authentication together with anti-replay protection should always be used. All 3GPP and fixed broadband traffic should pass through a SecGW before entering or leaving the security domain. When choosing a security gateway, the service provider can', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 172, 'parent\_id': '5dbd25cbf7554e1be5354758518f2991', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dc6c67468f57e86381546884e30a0ed4', 'text': 'go through the key points covered in the sections that follow to understand the capability of the SecGW and the requirements for the 5G network. Please note that not all the points in the following sections are mandatory, but it would be good to understand both the optional and mandatory requirements for SecGW before choosing any vendor.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 173, 'parent\_id': '5dbd25cbf7554e1be5354758518f2991', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5f6ec711bd2d3eb5b97cb2449b690063', 'text': 'Support of ESP', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 173, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9a3cf13ba950dfb5285047849df85cc3', 'text': 'ESP provides a mix of security services in IPv4 and IPv6. It can be applied alone or along with AH. The ESP header is inserted after the IP header and before the next layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode). ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality. The set of services provided depends on the option selected at the time of security association (SA) establishment and on the location of the implementation in a network topology.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 173, 'parent\_id': '5f6ec711bd2d3eb5b97cb2449b690063', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '46e26221cec7be5c7150c9d81f465ecd', 'text': 'The SecGW the service provider plans to deploy in the network should support ESP security protocol according to RFC 4303. Extended sequence numbers may be supported. For compatibility with earlier 3GPP releases, it is recommended to be backward compatible with nodes supporting only RFC 2406.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 173, 'parent\_id': '5f6ec711bd2d3eb5b97cb2449b690063', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3a6eeb63c8c9b6bfa32d01d9612e8459', 'text': 'Support of ESP Encryption Transforms', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 173, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '871e69009ff7979c570355f1b3754483', 'text': 'The SecGW should follow the implementation conformance requirements for ESP encryption transforms (including authenticated encryption transforms), as stated in RFC–8221.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 173, 'parent\_id': '3a6eeb63c8c9b6bfa32d01d9612e8459', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '297058f26921fb031ccbe02a9944dec7', 'text': 'Support of ESP Authentication Transforms', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 173, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '678498b990ac5798edb4fc19038dc21d', 'text': 'ESP should always be used to provide integrity, data origin authentication, and anti-replay services, and hence the NULL authentication algorithm is explicitly not allowed for use. Encryption without authentication is not effective and must not be used. IPsec offers three ways to provide both encryption and authentication:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 173, 'parent\_id': '297058f26921fb031ccbe02a9944dec7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd0da9633e45b357370f2547a40ac6458', 'text': '• ESP with an Authenticated Encryption with Associated Data (AEAD) cipher: This is the most modern method and handles encryption/decryption and authentication in single step. In this case, the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 173, 'parent\_id': '297058f26921fb031ccbe02a9944dec7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9e747756b5244d124930dff8871d1d5c', 'text': 'AEAD cipher is set as the encryption algorithm, and the authentication algorithm is set to none. Examples of this are ENCR\_AES\_GCM\_16 and ENCR\_CHACHA20\_POLY1305', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 174, 'parent\_id': '297058f26921fb031ccbe02a9944dec7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '754a9d1a511689cb8d5c9e1a3b10da59', 'text': '• ESP with a non-AEAD cipher + authentication: This is a traditional approach, where ESP is used with an encryption and an authentication algorithm. This approach is slower, as the data has to be processed twice: once for encryption/decryption and once for authentication. An example of this is ENCR\_AES\_CBC combined with AUTH\_HMAC\_SHA2\_512\_256.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 174, 'parent\_id': '297058f26921fb031ccbe02a9944dec7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a30c66252e04972f6268538d8b4d4da6', 'text': '• ESP with a non-AEAD cipher + AH (Authentication Header) with authentication: This is the slowest method and is not recommended. It also takes up more octets due to the double header of ESP+AH, which results in a smaller effective MTU for the encrypted data. With this method, ESP is only used for confidentiality without an authentication algorithm, and a second IPsec protocol of type AH is used for authentication. Examples of this are ESP with ENCR\_AES\_CBC and AH with AUTH\_HMAC\_SHA2\_512\_256.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 174, 'parent\_id': '297058f26921fb031ccbe02a9944dec7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6dd8acbc9acfeaa78a3515a828f08b67', 'text': 'The SecGW should also have mandatory support of ESP authentication algorithms specifically marked as “MUST” in RFC 8221.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 174, 'parent\_id': '297058f26921fb031ccbe02a9944dec7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a7ce1742e720252fa6133dde8501ed78', 'text': 'For the IoT use cases, the ESP Encryption Algorithm (ENCR\_AES\_CCM\_8) and ESP and AH Authentication Algorithm (AUTH\_AES\_XCBC\_96) need to be supported by the SecGW if the service provider has plans to deploy IoT as part of the network evolution. This might change as stronger and better algorithms emerge that are more suitable for a wide variety of CPU architectures and device deployments, ranging from high-end bulk encryption devices to small, low-power IoT devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 174, 'parent\_id': '297058f26921fb031ccbe02a9944dec7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3b2f488a788099cf740e183fb58b15bb', 'text': 'Requirements on the Construction of the Initialization Vector (IV)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 174, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8a254cff0252b3ad40d4d7fd948cf5d7', 'text': 'An initialization vector is a fixed-size input to a cryptographic algorithm. Its primary use is that of a nonce to ensure encrypting the same data with the same key does not result in the same ciphertext. In some cases, it might not be needed to transmit the IV because it can be derived from other information, such as the sequence number in ESP. Some algorithms require the IV to be random/unpredictable (for example, AES-CBC), but in many modern combined mode algorithms (for example, ChaCha20/Poly1305), it can just be a counter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 174, 'parent\_id': '3b2f488a788099cf740e183fb58b15bb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0ab0dd501b7837b356eb3f3450923b2f', 'text': 'The requirements for the IV construction for the IPsec deployed using SecGW are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': '3b2f488a788099cf740e183fb58b15bb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1094681213166b2ac6360010a993317c', 'text': '• For CBC mode: The IV field should be the same as the block size of the cipher algorithm being used. The IV should be chosen at random and should be unpredictable to any party other than the originator.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': '3b2f488a788099cf740e183fb58b15bb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '692ad086d82c297a6e3c3bd21734983c', 'text': '• For CTR, GCM, CCM, and GMAC mode: The IV field should be eight octets. The IV should be generated in a manner that ensures uniqueness. The same IV and key combination should not be used more than once. It is explicitly not allowed to construct the IV from the encrypted data of the preceding encryption process.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': '3b2f488a788099cf740e183fb58b15bb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'fbeced7577f6642869d1ac8afa48259c', 'text': 'Profiling of IKEv2 (Internet Key Exchange, Version 2)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9920c7e38c315ac9dd3c5f0dfbd6d567', 'text': 'The SecGW that’s planned to be deployed in the 5G network should support IKEv2 as defined in RFC 7296, “Internet Exchange Version 2 (IKEv2)” parameters. As stated in 3GPP 33.210, the following additional requirements apply for IKEv2:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bb28714136e48a89c05b5e149d1de3be', 'text': 'The following algorithms need mandatory support:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd5c0609753b63384ecba769ca8915184', 'text': '• Confidentiality: AES-GCM with a 16-octet ICV with a 256-bit key length', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '42c6a474f1212fd837ef0c3ab84d1834', 'text': '• Pseudo-random function: PRF\_HMAC\_SHA2\_384', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7be1b25b4df29938980fa6048b8b39dd', 'text': '• Diffie-Hellman group 20: 384-bit random ECP group', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b26873b6058998539440f21b72ff6fd6', 'text': 'The following algorithms should be supported:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '33ab88287abc5cc56e8cbc17a50eac89', 'text': '• Confidentiality: AES-GCM with a 16-octet ICV with a 128-bit key length', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'adc9ace60ed33089a04b138f8505baef', 'text': '• Pseudo-random function: PRF\_HMAC\_SHA2\_256', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e6acd2600edf4229002ecaed2bed7651', 'text': '• Integrity: AUTH\_HMAC\_SHA256\_128.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2316ae673d03157f310bdb7036fbc193', 'text': '• Diffie-Hellman group 19: 256-bit random ECP group', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8680e05895868b9395b3dc15ebc51a49', 'text': 'For IKE\_AUTH exchange:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f8071414a449cef8176e5d58e38bb6a9', 'text': '• Authentication Method 2 – Shared Key Message Integrity Code should be supported.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '584e95ba5eadd4060ff1c6c11c622bd8', 'text': '• IP addresses and fully qualified domain names (FQDNs) should be supported for identification.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 175, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '73fb5d2c08b9ac9efc4249699a25e280', 'text': '• Re-keying of IPsec SAs and IKE SAs should be supported as specified in RFC 7296.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 176, 'parent\_id': 'fbeced7577f6642869d1ac8afa48259c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '580f797ac6024d1c83766f9573a4f7d3', 'text': 'For the CREATE\_CHILD\_SA exchange:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 176, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a1bbe2b4f42fdbe369c12cc173c0207b', 'text': '• A DH key exchange should be used (giving Perfect Forward Secrecy) and the session keys should be changed frequently.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 176, 'parent\_id': '580f797ac6024d1c83766f9573a4f7d3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f80c29d1504f184d53e75f42c555f1b', 'text': 'For reauthentication:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 176, 'parent\_id': '580f797ac6024d1c83766f9573a4f7d3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '41e8bd601618eb456852997dd2b1815a', 'text': '• IKE SAs should be reauthenticated, as specified in RFC 7296.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 176, 'parent\_id': '580f797ac6024d1c83766f9573a4f7d3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b476b92bd8850f6e2abe4453dc49f44a', 'text': '• An NE should proactively initiate reauthentication of IKE SAs and the creation of child SAs (that is, the new SAs should be established before the old ones expire).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 176, 'parent\_id': '580f797ac6024d1c83766f9573a4f7d3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '952971465bc0fcdc282d199c4a8a6e41', 'text': '• An NE should destroy an IKE SA and its child SAs when the authentication lifetime of the IKE SA expires.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 176, 'parent\_id': '580f797ac6024d1c83766f9573a4f7d3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '512b17825d8a23dee33d6016cc5fa431', 'text': 'Support of IPsec Tunnel and Transport Mode', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 176, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ba32037d95d8bfc1696705cddb47585b', 'text': 'Before we discuss security gateway deployment modes, it is important to understand IPsec modes. IPsec can be configured in tunnel mode or transport mode:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 176, 'parent\_id': '512b17825d8a23dee33d6016cc5fa431', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd4a1374c686906c940a8da33b352f7f9', 'text': '• IPsec tunnel mode: In IPsec tunnel mode, the entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. In this mode the SecGW performs encryption on behalf of the hosts. The source SecGW encrypts packets and forwards them along the IPsec tunnel. The destination router decrypts the original IP datagram and forwards it on to the destination system. The major advantage of tunnel mode is that the end systems do not need to be modified to receive the benefits of IPsec. Tunnel mode also protects against traffic analysis; with tunnel mode, an attacker can only determine the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints. For inter-domain use cases, tunnel mode support for IPsec will be required and hence needs to be supported by the SecGW.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 176, 'parent\_id': '512b17825d8a23dee33d6016cc5fa431', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '05fd1fef36c7e85d748f6af989ddb4ca', 'text': '• IPsec transport mode: In IPsec transport mode, only the IP payload is encrypted, and the original IP headers are left intact. This mode has the advantage of adding only a few bytes to each packet. It also allows devices on the public network to see the final source and destination of the packet. With this capability, you can enable special processing (for', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 176, 'parent\_id': '512b17825d8a23dee33d6016cc5fa431', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd2c83b1e508241a76f03f464a7a466cb', 'text': 'example, QoS) on the intermediate network based on the information in the IP header. However, the Layer 4 header will be encrypted, thus limiting the examination of the packet. Unfortunately, transmitting the IP header in cleartext, transport mode allows an attacker to perform some traffic analysis. The option to use tunnel mode or transport mode is a design choice by the customer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 177, 'parent\_id': '512b17825d8a23dee33d6016cc5fa431', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'bd8da2e671889802229dac9c007c43f7', 'text': 'Security Gateway Deployment Modes', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 177, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b9815348486dec91f8e64fae8fa7903', 'text': 'There are basically two primary modes of deploying IPsec:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 177, 'parent\_id': 'bd8da2e671889802229dac9c007c43f7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bc92d374246791a6a0b75d61730f5a5b', 'text': '• Single tunnel concept or single child SA concept', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 177, 'parent\_id': 'bd8da2e671889802229dac9c007c43f7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e20babb2fb81b5bc91caefbae5049031', 'text': '• Multiple IPsec or multiple Child SA concept', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 177, 'parent\_id': 'bd8da2e671889802229dac9c007c43f7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '592df5168b335ecdd6d81f4439c555a6', 'text': 'In IPsec transmission between the eNB/gNB and SecGW, Internet Key Exchange (IKE) is used to create a security association. Before the encrypted traffic is sent or received, IKE version 2 (IKEv2) will create a second tunnel, an IKE security association (SA), which will be used for secure transmission of the child SA. This can be a single child SA or multiple child SAs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 177, 'parent\_id': 'bd8da2e671889802229dac9c007c43f7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed9eb9199388cce73a7cc084b642d537', 'text': 'The sections that follow discuss the single IPsec and multiple IPsec options.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 177, 'parent\_id': 'bd8da2e671889802229dac9c007c43f7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '91ca2ec8039bd7554d6d0e47cb338a87', 'text': 'Single Tunnel Concept or Single Child SA Concept', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 177, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f03608f490d45731d28342a8d903dca3', 'text': 'The use of single IPsec or multiple IPsec will depend on the network architecture. If all or multiple network functions are deployed in the same location, you will use a single IPsec tunnel to encrypt the traffic toward the destination. You can then configure internal VRFs (IVRFs) to route the traffic between the different VRFs, as shown in Figure 4-13, which illustrates the single tunnel concept.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 177, 'parent\_id': '91ca2ec8039bd7554d6d0e47cb338a87', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '6f3eeabfe3c3b77b503253054be8efb2', 'text': '((A>) OAM Vrf - OAM Vrf - X2 X2 Vi - 81 St Vrf = Xn, Xx Xn, Xx Vrf = N2 N2 Vrf-N3 N @ IPsec backhaul', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 178, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8510fd3410cdaaff0f35d354b8c36179', 'text': 'Figure 4-13 Single IPsec Tunnel Mode Concept', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 178, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '523a5c09cb7d45f908e2106d5de43665', 'text': 'Here are the key points:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 178, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5e6de1cf48843632a3c548867ce3407e', 'text': '• All traffic, such as OAM, S1-C, S1-U, X2-C, X2-U, Xn-C, Xn-U, Xx-C, and Xx-U, traverses the same tunnel.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 178, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b92247d7763203228d14f0ba024ed77c', 'text': '• It’s difficult to change the architecture in later phases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 178, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'cc08a2f4e99b6f93e89ead36ba41db8e', 'text': 'Note', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 178, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8320ae1772f51311ad9da952782af9f4', 'text': 'Based on my experience of deploying SecGWs with many service providers, the following details are worth knowing beforehand:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 178, 'parent\_id': 'cc08a2f4e99b6f93e89ead36ba41db8e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fa0d13f76f8c6ede45f2b9bd82460260', 'text': '• Some RAN vendor radio base stations (eNBs) support single tunnel for everything. In such situations, it would be recommended to have management (OAM) on SSL/SSH and not IPsec for troubleshooting, as maintenance would not be possible if the tunnel is not up.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 178, 'parent\_id': 'cc08a2f4e99b6f93e89ead36ba41db8e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67804650ea4332dda0af034e4c600689', 'text': '• Some RAN vendor radio base stations (eNBs) will support two tunnels: the first tunnel for X2 and S1 and the second tunnel for OAM. Therefore, there’s no need to configure SSL/SSH for troubleshooting/maintenance purposes.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 178, 'parent\_id': 'cc08a2f4e99b6f93e89ead36ba41db8e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '12723520c4098413e27a75fa33745a3b', 'text': 'Multiple IPsec or Multiple Child SA Concept', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 178, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '75f730dfcc3cf84e278aa4cc153335d2', 'text': 'Multiple IPsec deployments are mostly used in an enterprise architecture where you need to connect multiple enterprise branches to the enterprise’s headquarters. In service provider telco deployments, multiple IPsec will be used if you have a very distributed architecture where each of the network functions needs separate SecGWs or multiple instances of SecGWs catering for each of the components. Figure 4-14 illustrates an example of the multiple IPsec tunnel mode where a context within a SecGW is dedicated to a network function.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 179, 'parent\_id': '12723520c4098413e27a75fa33745a3b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '21e4abd4a6aa827310f89ec76b7ce645', 'text': '¥ Vrf - OAM Vrf - X2 X2 S1 Vrf - 81 Xn, Xx Vrf = Xn, Xx N2 Vrf - N2 N3 Vrf—N3 IPsec backhaul', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 179, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'efbdde18207905edf4eab3aa2a4dea6c', 'text': 'Figure 4-14 Multiple IPsec Tunnel Mode Concept', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 179, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '00009bae5a3800437fddb66e2b830ab9', 'text': 'Having the option of configuring multiple contexts, which allows a single SecGW to behave like multiple standalone SecGWs with options of dedicated interfaces or shared interfaces, will provide you the flexibility to use a single SecGW as multiple standalone SecGWs to enable multiple IPsec deployment, as shown in Figure 4-14.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 179, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f657b25adf80e2f0aa6e66187946c18b', 'text': 'Here are the key points:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 179, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8339a06b0ae61672364ec758b4326560', 'text': '• Different traffic types traverse different tunnels/SAs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 179, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f8104599c7221dd4d09883640bd41808', 'text': '• Traffic separation is based on tunnels/SAs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 179, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b4cf035e63220071aa6602ce3ea85092', 'text': '• Multiple IPsec tunnels increase IKE SAs and the number of outer IP addresses.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 179, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1fd8a29fbac6e147219bccce55f68fa7', 'text': 'Security Gateway in 4G and 5G Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 179, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '73484f9a67b848683eaa1ff2e4501e3c', 'text': 'This section provides the service provider with information on how the SecGW solution could cater for 4G and 5G deployment use cases. The section starts with the 4G use cases to help you understand the evolution of the security gateway control from 4G to 5G without having to make major changes in the design or replacing the existing centralized SecGW deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 180, 'parent\_id': '1fd8a29fbac6e147219bccce55f68fa7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '823725efd60ca5726736f0da3f854419', 'text': '4G Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 180, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '59720b912261bf54e08c3147c318f01b', 'text': 'Many of the service providers who own their own back haul were used to not deploying a SecGW as the eNB network element (NE), and the Evolved Packet Core (EPC) was considered to be in the same trusted secure domain. But in recent times, there has been a surge in threat actors trying to connect rogue NE nodes toward the packet core. Apart from the threat vector of rogue NEs, many service providers have some NEs passing through the non-trusted insecure transport network domain owned by another service provider.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 180, 'parent\_id': '823725efd60ca5726736f0da3f854419', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5d1833351bd63cb9943e3b48e851e57c', 'text': 'Deploying IPsec using SecGW will provide authentication and encryption between the eNB and the packet core nodes, thereby securing the back haul. The key interfaces that the SecGW would secure are the S1 and X2 interfaces. The SecGW can be deployed as centralized or distributed, depending on whether you have deployed centralized 4G or Control Plane User Plane Separated (CUPS) 4G. In some cases, both centralized and distributed deployments of a SecGW need to be deployed, as you might have S1 and X2 terminating in the edge site as well as the centralized packet core in some instances. The section “4G CUPS Network” discusses distributed SecGW deployment in more detail.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 180, 'parent\_id': '823725efd60ca5726736f0da3f854419', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '081784d82061b4a97473f6504d3e3693', 'text': 'Figure 4-15 shows the option of a centralized security gateway, where the S1 interface and X2 interface are secured using the security gateway. In this case, both the S1 interface and the X2 interface are terminated in the centralized security gateway, which is located in the centralized 4G Evolved Packet Core (EPC) location.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 180, 'parent\_id': '823725efd60ca5726736f0da3f854419', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a7528f47871b61814b6174e3f3f65853', 'text': '; o= Centralized EPC (A) §1,X2 < 4G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 181, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dd8ea76d45bceca172fc38e6ff1b16b2', 'text': 'Figure 4-15 Securing S1 and X2 Interface Using Security Gateway', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 181, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd01e889f0c42a29509c59bad79d4b844', 'text': 'The SecGW might require large pools of IPsec capability depending on the network size of the service provider and should also be able to statefully inspect the traffic entering and leaving the tunnel. This device might also be positioned in a geographically dispersed environment if stateful inspection is required and configured in different resiliency modes (Active/Standby, Active/Active, and so on). Figure 4-16 illustrates the IPsec tunnel mode deployment for a centralized 4G SecGW deployment, which protects the S1, X2, and OAM interfaces. Once the tunnel is terminated in the SecGW at the central DC location, it can then be routed to MME and SGW. In actual deployments, IPsec tunnels are mapped to Virtual Routing and Forwarding (VRF) instances using a single public IP address. When an IPsec-encapsulated packet arrives at the SecGW from the eNB, IPsec performs security association (SA) lookup for the Security Parameter Index (SPI), destination, and protocol. The packet is decapsulated using the SA, gets associated with the inside VRF (IVRF), and is forwarded using the IVRF routing table.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 181, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '856defbe43470a442b7a1b3ddf4a585d', 'text': 'B Element Management System of RAN vendor (<A>) Vrf - OAM OAM X2 Vrf - X2 S1 Vrf- 81 EPC (SGW, MME) eNodeB (4G) IPsec backhaul ECEUE e e o] Central DC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 182, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a201e1512a0f11763be0922d1050518a', 'text': 'Figure 4-16 Detailed View for Securing S1 and X2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 182, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6370ffe9b3ab2ba228cbf109d1855a7e', 'text': 'The deployment of the SecGW in the centralized deployment mode should provide the security controls mentioned in Table 4-1 and the service provider could choose what traffic (CP only, CP + UP) is required to be secured. Normally in traditional 4G deployment configurations, it’s difficult to separate the CP and the UP traffic, unless CUPS is deployed. The section “4G CUPS Network,” later in the chapter, discusses this in more detail.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 182, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '64d1c501385057c4729c2c6fd169b60c', 'text': 'As Figure 4-17 illustrates, the SecGW routes the S1-C traffic to MME and S1- U traffic to SGW. In some cases, such as shared sites between service providers, NAT might be used along with routing to provide topology hiding.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 182, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd41bd0342f503ad8294c3c329cb29bfb', 'text': '((A>) §1-C OAM X2 St S1-U eNodeB IPsec backhaul (4G)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 182, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '85d66bd4c5c2780fae98a05b661ead90', 'text': 'Figure 4-17 Routing of S1-C to MME and S1-U to SGW Using SecGW', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 182, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8570736073636ffd4ed91df572e5e430', 'text': 'Table 4-1 outlines the security controls per interface in centralized 4G deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 183, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '9f9a639e065059bf6a45577861a6ad0b', 'text': 'Interface Access Node Security o Control OAM ¢NB [Psec S1-C eNB MME IPsec S1-U ¢NB SGW [Psec X2-C eNB <>¢eNB IPsec X2-U i ¢eNB <>¢NB [Psec', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Interface</th><th>Access Node L</th><th></th><th>Security Control</th></tr></thead><tbody><tr><td>OAM</td><td>¢NB</td><td></td><td>[Psec</td></tr><tr><td>S1-C</td><td>eNB</td><td>MME</td><td>IPsec</td></tr><tr><td>S1-U</td><td>¢NB</td><td>SGW</td><td>[Psec</td></tr><tr><td>X2-C</td><td>eNB &lt;&gt;¢eNB i</td><td></td><td>IPsec</td></tr><tr><td>X2-U</td><td>¢NB &lt;&gt;¢NB</td><td></td><td>[Psec =</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 183, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fd0def02261ee5376a3d801f94980bf9', 'text': 'Table 4-1 Security Controls per Interface—4G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 183, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6e60396af6a8116180e37bf0c6bbadd6', 'text': 'If the RAN vendors support single tunnel for everything, it is recommended that you have management (OAM) on SSL/SSH and not IPsec for troubleshooting, as maintenance would not be possible if the tunnel is not up. If OAM is not protected using IPsec, then mechanisms such as NETCONF/TLS with PKIX for certificate-based mutual authentication or PKIX-based SSHv2 should be implemented. Granular access controls should also be implemented to enhance the OAM access control, as discussed later in the chapter in the section “Granular Access Control.”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 183, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7baf03b9284bbfe5638ff76692d0dfe6', 'text': '4G CUPS Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 183, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '179731c20bbd29053fd2f3fd6d7d80c2', 'text': '4G CUPS brings in Control Plane User Plane Separation (CUPS) and can be deployed as a co-located CUPS or distributed CUPS. 4G CUPS based on the Packet Forwarding Control Plane (PFCP) protocol was implemented to enable the following functions:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 183, 'parent\_id': '7baf03b9284bbfe5638ff76692d0dfe6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0eadbacdaff8c3f6463a700f3995cd4f', 'text': '• Reduced latency on application service (for example, by selecting user plane nodes that are closer to the RAN or more appropriate for the intended UE usage type without increasing the number of control plane nodes).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 183, 'parent\_id': '7baf03b9284bbfe5638ff76692d0dfe6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a4478c47fd54088bcde4562541bd62dd', 'text': '• Support for an increase of data traffic by enabling the addition of user plane nodes without changing the number of SGW-C, PGW-C, and TDF-', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 183, 'parent\_id': '7baf03b9284bbfe5638ff76692d0dfe6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'deacb92dede5ae0f48457645448a2ab0', 'text': 'C in the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 184, 'parent\_id': '7baf03b9284bbfe5638ff76692d0dfe6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8abb5dc7c5f7b684b1c57cb60f464b59', 'text': '• Locating and scaling the CP and UP resources of the EPC nodes independently.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 184, 'parent\_id': '7baf03b9284bbfe5638ff76692d0dfe6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '17898a52b5b50c5063d5cc58d5f839fd', 'text': '• Independent evolution of the CP and UP functions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 184, 'parent\_id': '7baf03b9284bbfe5638ff76692d0dfe6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '923f69eb585934af96073af5045bfa75', 'text': '• Enabling SDN to deliver user plane data more efficiently.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 184, 'parent\_id': '7baf03b9284bbfe5638ff76692d0dfe6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3a905eccdabe7f397efe757756b6a26e', 'text': 'The SecGW deployment in co-located CUPS mode is similar to the deployment of EPC in non-CUPS mode, as the control plane and user plane, though separated, still exist in the same location or the same DC (data center). In distributed CUPS, the control plane and user plane are not only separated, but also distributed and deployed in edge data centers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 184, 'parent\_id': '7baf03b9284bbfe5638ff76692d0dfe6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9e2666369c9ff154fd4873b0e18c59e1', 'text': 'Figure 4-18 shows the distributed deployment of 4G CUPS, where the user plane (UP) is deployed toward the edge to cater for the latency-sensitive use cases, whereas the UP for use cases where latency is not an issue as well as the control plane (CP) is deployed in the centralized 5GC DC. CUPS introduces three new interfaces—Sxa, Sxb and Sxc—between the CP and UP functions of the SGW, PGW and TDF, respectively, which is collectively stated as Sx in the figure and is protected by the IPsec ESP and IKEv2 certificate-based authentication provided by the SecGW.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 184, 'parent\_id': '7baf03b9284bbfe5638ff76692d0dfe6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '8a06984ef5f86384e95b5b121829be2d', 'text': 'Centralised “,— Distributed SecGW S1, X2, Sx SecGW 4 o= 4G CUPS ((A)) Shxe o - ——— e N\\ == 10 <« Distributed User \\ | = - Plane Centralized EP! i 4\\ (p) S1,X2 MEC 4G (A)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 184, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1453e6993edfed4475afb3a4495bb9e5', 'text': 'Figure 4-18 Evolution of SecGW Architecture to Secure 4G CUPS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 184, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bfc7073c6dd1fe3c7f41e0065f631741', 'text': 'As Figure 4-19 illustrates, the S1-U from the eNB can be terminated in the distributed SecGW deployed in the MEC, and S1-C from the eNB is terminated in the centralized SecGW, which will then forward the packets to the SGW-C after decryption. X2, although also shown as being terminated in the centralized SecGW location, can also be deployed on the MEC layer, which is purely the service provider’s choice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 184, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b1123f6367150d92075caec2c887551a', 'text': 'e e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 185, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '20e5a51b82f9a06347d6cd0ed3f52c69', 'text': 'e f Element Management System of RAN vendor ((A>) OAM Vii - OAM X2 Vi - X2 §1-C Vi - $1-C (MME) . Sx Vi —Sx(SGW ~C / W-C, TDF-C) St-U L S ——— Central DC | IPsec o | tunnel Vii-§1-U Sx SGW-U/PGW-U/TDF-U|! \\ e MEC e Gi', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 185, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd14cf3ba2d79197b42d49af06ca2f698', 'text': 'Figure 4-19 Detailed View for Securing Distributed 4G CUPS Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 185, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '21d2ae4f615c4fed107228b6124c58de', 'text': 'Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 185, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e16cffe74e4186e7032882ba78b4522e', 'text': 'In the CUPS, the deployment of the SecGW in the centralized and distributed mode would secure the Access and Packet Core nodes described in Table 4-2 using the IPsec ESP and IKEv2 certificate-based authentication.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 185, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '28b2f10b0eb18ba164c22a4aefac5416', 'text': 'Interface Access Node Security Control L OAM eNB [Psec X2-C eNB [Psec X2-U eNB [Psec S1-C eNB MME [Psec S1-U eNB [Psec Sxa [Psec Sxb [Psec Sxc [Psec', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Interface</th></tr></thead><tbody><tr><td>OAM</td></tr><tr><td>X2-C</td></tr><tr><td>X2-U</td></tr><tr><td>S1-C</td></tr><tr><td>S1-U</td></tr><tr><td>Sxa</td></tr><tr><td>Sxb</td></tr><tr><td>Sxc</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 186, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fda2f8044b6c80c2122fae464799daaf', 'text': 'Table 4-2 Security Controls per Interface—4G CUPS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 186, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1d4a0496561b1860823f7f5efd8c598d', 'text': '5G NSA (Non-Standalone) Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 186, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'df895ef41610507271889500ef405068', 'text': 'Multiple deployment options are available for the 5G Non-Standalone (NSA) model. One of the NSA options is Option 3, where the RAN is composed of a master node and secondary node. The master node is LTE eNB, the secondary node is New Radio (NR) en-gNB, and the packet core is EPC (4G packet core). NSA Option 3 supports legacy 4G devices, and the 5G devices only need to support NR protocols. The 5G NSA options are purely the choice of the service provider, as you might chose to skip 5G NSA and deploy 5G SA directly. Most of the 5G NSA options are based on the software upgrade on the eNB and the EPC to allow higher throughput capabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 186, 'parent\_id': '1d4a0496561b1860823f7f5efd8c598d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5ace2ef8c0e08152e68195abf113339a', 'text': 'Figure 4-20 shows you the different interfaces in the network when you have a multi-RAT (radio access technology) deployment, such as 4G, 4G CUPS, and 5G NSA deployed in the network. The packet core might consist of an upgraded 4G packet core or some elements of the 5G core, depending on the 5G NSA model deployed. As you can see from the figure, the complexity of securing the network increases with the deployment of multi-RAT in your network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 186, 'parent\_id': '1d4a0496561b1860823f7f5efd8c598d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '2a44f56cf1dd94c75d4470e2634f03a4', 'text': 'o e e 5G NSA A Xx, Xn, N2, N3 Xx N2, N4 ; S1, X2, Sx 4G CUPS A 81,2 | I- B dem e s e Centralized EPC & 5GC : it ot i MEC 4G A', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 187, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6790196106493a32dd03166f6b7a4abc', 'text': 'Figure 4-20 Evolution of SecGW Architecture to Secure 5G NSA Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 187, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ceb7c38b8285053f8d7d413665bd8800', 'text': 'As Figure 4-21 illustrates, the deployment of the SecGW in the centralized and distributed mode would secure the Access and Packet Core nodes described in Table 4-3 using the IPsec ESP and IKEv2 certificate-based authentication in 5G NSA and multi-RAT deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 187, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'e194c0b2e9425d8cb4d6033f95b47400', 'text': 'S Element Management System of (<A>) RAN vendor OAM Vrf - OAM x2,xn @ Vrt=X2, Xn EPC +5GC sic.ne @ Vit-81-C, N2 Vrf - N4 (SMF) B ~ Sx,N4 j= N3 Central DC IPsec e s e S i e e e tunnel Vrt=N3 Sx, N4 UPF, SGW-U, PGW -U % i TN F— MEC Gi/N6', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 187, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9e23d72bf3cbbe87983f2c2dd6e9af73', 'text': 'Figure 4-21 Detailed View for Securing NSA Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 188, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '07b1ba2370841de73c027785ae8ad396', 'text': 'Interface Access Node Core Node Security Control OAM eNB NMS/EMS [Psec X2-C eNB - eNB [Psec X2-U eNB - eNB IPsec ¢NB - ngNB S1-C eNB MME IPsec S1-U eNB SGW-U [Psec Sxa SGW-U-8GW-C [Psec Sxb PGW-U-PGW-C [Psec Sxc TDF-U - TDF-C IPsec Xn-C IPsec ¢NB - gNB Xn-U ¢NB - gNB IPsec N2 eNB AMF IPsec N3 eNB UPF IPsec N4 UPF - SMF IPsec', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Interface</th><th>Access Node</th><th>Core Node</th><th>Security Control</th></tr></thead><tbody><tr><td>0AM</td><td>eNB</td><td>NMS/EMS</td><td>[Psec</td></tr><tr><td>X2-C</td><td>eNB - eNB</td><td></td><td>[Psec</td></tr><tr><td>X2-U</td><td>eNB - eNB ¢NB - ngNB</td><td></td><td>IPsec</td></tr><tr><td>S1-C</td><td>eNB</td><td>MME</td><td>IPsec</td></tr><tr><td>S1-U</td><td>eNB</td><td>SGW-U</td><td>[Psec</td></tr><tr><td>Sxa</td><td></td><td>SGW-U - SGW-C</td><td>[Psec</td></tr><tr><td>Sxb</td><td></td><td>PGW-U-PGW-C</td><td>[Psec</td></tr><tr><td>Sxc</td><td></td><td>TDF-U - TDF-C</td><td>IPsec</td></tr><tr><td>Xn-C</td><td>¢NB - ¢gNB</td><td></td><td>IPsec</td></tr><tr><td>Xn-U</td><td>¢NB - gNB</td><td></td><td>IPsec</td></tr><tr><td>N2</td><td>eNB</td><td>AMF</td><td>IPsec</td></tr><tr><td>N3</td><td>¢NB</td><td>UPF</td><td>IPsec</td></tr><tr><td>N4</td><td></td><td>UPF - SMF</td><td>IPsec</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 188, 'parent\_id': '9e23d72bf3cbbe87983f2c2dd6e9af73', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5fb5405de3b6990edf343036abe0d87e', 'text': 'Table 4-3 Security Controls per Interface—NSA', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 188, 'parent\_id': '9e23d72bf3cbbe87983f2c2dd6e9af73', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4083a046f17103e0fe6e1c530681d916', 'text': '5G Standalone (SA) Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 188, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '92ce12b40241f904fb8d3fb4fe8d36d7', 'text': 'The 5G SA packet core is equipped with several new capabilities inherently built into it so that operators have the flexibility and capability to face new', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 188, 'parent\_id': '4083a046f17103e0fe6e1c530681d916', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '25834d41806b9f8217a572f9c64b5c34', 'text': 'challenges presented by the new set of requirements for various new use cases. The network functions in the new 5G core are broken down into smaller entities, such as the Session Management Function (SMF) and User Plane Function (UPF), which can be used on a per-service basis. Gone are the days of huge network boxes; welcome to services that automatically register and configure themselves over the Service-Based Architecture, which is built with the new functions like the Network Repository Function (NRF) that borrow their capabilities from cloud-native technologies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 189, 'parent\_id': '4083a046f17103e0fe6e1c530681d916', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '76755b4c3721bebfb93c16c5e2545780', 'text': 'In 5G SA, the control plane and the user plane from the 5G radio node (gNB) are terminated in the 5GC. There is no dependency on the 4G infrastructure, such as eNB or EPC. This allows for the complete virtualization of the entire packet core stack for 5G, which can be separate from the 4G packet core (EPC) as illustrated in Figure 4-22.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 189, 'parent\_id': '4083a046f17103e0fe6e1c530681d916', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '14b5f093bc82698cdcfc19deb85b7450', 'text': 'o ((A)) Xn, N2, N3 Xn 5G NSA (A) Xx, Xn, N2, N3 Xx N2, N4 560P S6UP S1, X2, Sx 46 cups(( A)) S1.%2 SIS T g s l4aup soup ~ = - Centralized 5GC X2 = and EPC MEC s ((A)) L st', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 189, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '386e80068135cf3b9290f54665be6173', 'text': 'Figure 4-22 Evolution of SecGW Architecture to Secure 5G SA', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 189, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c8befeff582177e50d545183546c241f', 'text': 'As Figure 4-23 illustrates, the deployment of the SecGW in the centralized and distributed mode would secure the Access and Packet Core nodes described in Table 4-4 using the IPsec ESP and IKEv2 certificate-based authentication in 5G SA and multi-RAT deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 189, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '4bc02cfe1f05da17aef7380ad7a1822c', 'text': 'e RAN vendor Element Management System of (<A>) OAM Vi - OAM Vit = Xn, Xx N2 (AMF) LS - Vrf - N4 (SMF) | Xn, Xx e e e e e e e e e Central DC Vrf-N3 N4 Xn, Xx UPF i MEC Tn P — (<A>)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 190, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fb0a72896102013ea32eb78d62f26a80', 'text': 'Figure 4-23 Detailed View for Securing SA Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 190, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '8a117fb88f4ea7f8a2fae9c3c84858b3', 'text': 'Interface OAM eNB X2-C ¢eNB - eNB eNB -eNB X2-U S1-C eNB SI-U eNB Sxa Sxb Sxc Xn-C oNB - gNB Xn-U oNB - gNB N2 gNB N3 gNB N4', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Interface</th><th></th></tr></thead><tbody><tr><td>O0AM</td><td>eNB</td></tr><tr><td>X2-C</td><td>¢eNB - eNB</td></tr><tr><td>X2-U</td><td>eNB -¢eNB</td></tr><tr><td>SI-C</td><td>eNB</td></tr><tr><td>SI-U</td><td>eNB</td></tr><tr><td>Sxa</td><td></td></tr><tr><td>Sxb</td><td></td></tr><tr><td>Sxc</td><td></td></tr><tr><td>Xn-C</td><td>gNB - gNB</td></tr><tr><td>Xn-U</td><td>gNB - gNB</td></tr><tr><td>N2</td><td>gNB</td></tr><tr><td>N3</td><td>gNB</td></tr><tr><td>N4</td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 191, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '86b1d113e0b721cb8a5253f17c84b4bf', 'text': 'Table 4-4 Security Controls Per Interface—4G Toward NSA', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 191, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '362d79c31d5c99efcefa3cc8d3ea36b9', 'text': 'VRAN (Virtualized RAN), O-RAN (Open RAN), and C-RAN (Cloud RAN) Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 191, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c23beafd1ae4ddea87b4cd14f1f6d240', 'text': 'Before we get into the details of O-RAN specifically, let’s discuss the differences between VRAN, O-RAN, and C-RAN. These terms are used in conjunction with each other, and though they are closely linked together, there are some differences between them.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 191, 'parent\_id': '362d79c31d5c99efcefa3cc8d3ea36b9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f265ab4b476c31265246a134896d7d0c', 'text': 'Virtualized RAN (VRAN) relates to the decomposition of software from hardware and provides you with virtualized 5G network functions that can be deployed in an x86 server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 192, 'parent\_id': '362d79c31d5c99efcefa3cc8d3ea36b9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bc2a21a64abf194d60d9dc34843b9ca7', 'text': 'Open RAN (O-RAN), which is specified by the O-RAN Alliance, provides you with openness, enabling you to choose different vendors for Radio Resource Unit (RRU), Distributed Unit (DU), and Centralized Unit (CU). The DU and CU can be Virtualized RAN (VRAN) functions or can be deployed as custom- built hardware. So, in theory, you can further split O-RAN into O-RAN based on VRAN and O-RAN based on bare metal (BM).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 192, 'parent\_id': '362d79c31d5c99efcefa3cc8d3ea36b9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '387a62531f47ce0adc70ec4896dbf34b', 'text': 'Cloud RAN (C-RAN), which is also sometimes referred to as Centralized RAN, has the Base Band Unit (BBU) deployed at a centralized location, which enables you with a lightweight deployment of RRU and Antenna at the cell site. C-RAN architectures use a front-haul interface between the BBU in the centralized core and the RRU in the cell site. Most service providers are looking at O-RAN deployments with or without VRAN, as compared to C- RAN deployments specifically, due to the flexibility provided by O-RAN architectures, such as flexibility in deploying CU and DU based on use cases and cost optimization due to different vendor selection for RRU, DU, and CU. This section will discuss O-RAN deployments based on VRAN and BM as well as the open front-haul interface related to both O-RAN and C-RAN.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 192, 'parent\_id': '362d79c31d5c99efcefa3cc8d3ea36b9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '32f5e1b9311d99c2502e70a8f1d3fac6', 'text': 'The O-RAN approach is a modular strategy for designing and building networks that combine the optionality of open interfaces and a robust ecosystem with cloud-scale economics. Following 3GPP architectural principles and leveraging standards being defined by the O-RAN Alliance, the monolithic base station is decomposed into functional elements interconnected by open interfaces. Disaggregation (the decoupling of software and hardware) is maximized to allow the deployment of radio signal processing software in a cloud or mini-cloud environment. The combination of these principles allows operators to utilize a far more diverse supply chain to build an architecture that scales like cloud systems instead of hardware appliances. Modular software solutions enable automation across the full lifecycle, from deployment to management and operations. Figure 4-24 illustrates the O-RAN logical architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 192, 'parent\_id': '362d79c31d5c99efcefa3cc8d3ea36b9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '34c89eb61e16ded8a27ccfe8b1a56817', 'text': "ST Service management and Orchestration Framework 3GPP Interfaces [— \_\_ O-RAN Interfaces 01 Al 02 01 E2 Near-Real-Time RAN Intelligent Controller E2 ceemscsscscccecccmeennh - e e e e s e X2-c X2-u O-eNB E1 ceemesmmcbecen——- Xn-u . 0-CU-UP NG-u i i e e i e Xn-¢ Open Fic | S pececsceciccccccnnan NG-¢ Fronthaul ' F1-u M-Plane 0-DU Open Fronthaul Open Fronthaul CUS-Plane M-Plane O-RU", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 193, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'text': 'Figure 4-24 Logical O-RAN Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 193, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ae63375fc3dab1702e673d1da99ffe61', 'text': 'As shown in Figure 4-24, the O-RAN architecture includes 3GPP interfaces and the following new interfaces related to O-RAN:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 193, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '44b1bd683a9c743a28f6e884fe24f095', 'text': '• 3GPP interfaces: X2 control and user planes, Next Generation (NG) control and user planes, E1 control and user planes, and F1 control and user planes.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 193, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '00ad9df1c7b239bb76f2f2966a8de1f0', 'text': '• O-RAN interfaces: O1, O2, A1, E2, Open Front Haul (FH) control plane, user plane, and synchronization plane (CUS-Plane), and Open FH M- plane.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 193, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '40bf595e4dffe77cb0cd3978f9e044f7', 'text': '• Near-real-time RAN Intelligent Controller: Enables near-real-time control and optimization of O-RAN elements and resources via fine- grained data collection and actions over the E2 interface.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 193, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'de5adb17042e34cf68e1cea040420118', 'text': '• Non-real-time RAN Intelligent Controller: Enables non-real-time control and optimization of RAN elements and resources, AI/ML', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 193, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '843d1bbb1203687bfd8dcad9b8e17007', 'text': 'workflow (including model training and updates), and policy-based guidance of applications/features in near-RT RIC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 194, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6e1782597b0bc4db124d4cea1533cd32', 'text': '• O-RAN Central Unit – Control Plane (O-CU-CP): A logical node hosting the RRC and the control plane part of the Packet Data Convergence Protocol (PDCP).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 194, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '42475c7c7ea18353fbaa9391a5709b6d', 'text': '• O-RAN Central Unit – User Plane (O-CU-UP): A logical node hosting the user plane part of the Packet Data Convergence Protocol (PDCP) and the Service Data Adaptation Protocol (SDAP).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 194, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8beeb2e4b4b29bfc2a9a18d4a32a8b48', 'text': '• O-RAN Radio Unit (O-RU): A logical node hosting Low-PHY layer and RF processing based on a lower-layer functional split.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 194, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '599a5e5ccf8a06374e5c010cb9f551d2', 'text': '• O1: Interface between management entities in Service Management and Orchestration Framework and O-RAN-managed elements, for operation and management.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 194, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5143455edee858e7897f5d9e88185e74', 'text': '• xAPP: Independent software plug-in to the near-RT RIC platform to provide functional extensibility to the RAN by third parties.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 194, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bf87dcbc13ecf8d8b78e9e3e24b914bb', 'text': 'Apart from the aforementioned new interfaces, O-RAN also introduces the following new functions and frameworks:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 194, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '677cdadf3986e4b6daf7c5f4c40a79c6', 'text': '• O-Cloud: O-Cloud is used to host the network functions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 194, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cce7b29a986475c89fe0302c152c0149', 'text': '• Services Management and Orchestration Framework (SMO): SMO manages the network functions and O-Cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 194, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '84b421adc3212526f6c5dfdc2290ce70', 'text': '• Non-real time and near-real time RAN Intelligent Controller (RIC): RIC provides mobility management, admission control, and interference management as x-Apps (near-real-time RIC) or r-Apps (non-real-time RIC) on the northbound interface and enforces network policies via a southbound interface toward the radios.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 194, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f48f71aa8b52971129f3dde8b78edad5', 'text': 'The network functions using these interfaces, as well as the security controls to secure these interfaces, are discussed later in Table 4-5.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 194, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6b10a7d6efea6bbde9684ab4a43c5b3b', 'text': 'With the introduction of 5G, the industry acknowledged that networks need to be built in a more efficient, scalable, and automated way, and that included the RAN components as well. As a result, the RAN architecture is evolving from a static, monolithic, highly proprietary architecture to a cloud-based architecture, O-RAN/VRAN. O-RAN architecture incorporates key technology trends into the RAN space, such as the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 194, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '75527352b7bbe4b60c5519f38c387172', 'text': '• Decomposing the Base Band Unit (BBU) monolithic block into sub- functions, Distributed Unit (DU) and Central Unit (CU), and allowing them to be centralized and flexibly placed', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 195, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9a1a389b6bb0bc80808b517dbbff2739', 'text': '• Disaggregating and virtualizing those subfunctions, enabling RAN components to run on a NFVi infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 195, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c308ce98a23dd1ef78eb6ccdb941474d', 'text': '• Using fully standardized and open interfaces to enable a truly multi-vendor RAN system', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 195, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5a08b19f1b61247a855d9f72f5a80354', 'text': 'The benefits that can be derived from this new architecture are multiple. The open multivendor system promotes competition, innovation, diversity of use cases, and time-to-market (TTM) availability of products. Additionally, the technical benefits provided by the O-RAN architecture translate into effective cost savings, namely the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 195, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '562ab86c2cd9a4cf16654ccc8ee80f6c', 'text': '• The centralization of DU and CU RAN functions simplify the cell site and, with it, reduce the cost of building the site and the recurrent cost associated with it, such as power and rent. Building so-called skinny sites also increases the number of sites that qualify as a cell sites, which is critical for 5G high-density deployments, which translates into operational efficiencies and TTM.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 195, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0d11cf350e75b5849a61bb173c84103a', 'text': '• Centralization of RAN functions also enable better use of RF resources while improving the service to the users.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 195, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f0afa122dec02244e9e5b4ca14ddfedf', 'text': '• Virtualization adds the benefits of hardware (HW) pooling, dynamic resource allocation, and improved resiliency and redundancy in the RAN (which is critical for some SLAs)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 195, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cff11d520a6faf2b27d57849a42a5a3f', 'text': '• Centralized and virtualized components with open/standard interfaces provide the baseline for full RAN system automation, where multiple vendors and multiple domains can be jointly automated by the same cross- domain automation system for the same service flow (for example, scalable and fast RAN site deployment, scalable upgrades, central monitoring, real-time visibility, and closed-loop operations). Automation is key for accelerated network deployment/network changes and service level assurance.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 195, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6adb282ae24d04ed1148f5a14ee49d62', 'text': '• O-RAN/VRAN architecture provides a future-proof foundation for critical RAN developments, such as RAN network slicing support with flexible resource allocation and node/function placement per slice type. This can', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 195, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '09524c6cfb075b1a7ef10f2bbbff58a8', 'text': 'only be achieved by RAN systems that are built to provide cloud-like flexibility.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 196, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0c2b92809e80fe41fb4a8c8b099780b5', 'text': '• Network functions such as the near-real-time RIC, O-CU-CP, O-CU-UP, and O-DU implemented as containerized microservices can leverage cloud-native security advances such as hardware resource isolation, automatic reconfiguration, and automated security testing, which can improve both open source vulnerability management and security configuration management.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 196, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6fe706f7079d1819e3dd14668d41ea3a', 'text': 'As described in the preceding list, the RAN BBU component is disaggregated into the DU and the CU and can be deployed in far-edge and edge DCs, as per the network requirement. The O-RAN architecture brings in new interfaces— notably the F1 interface between gNB-DU and gNB-CU, the E1 interface between gNB-CU-CP and gNB-CU-UP, and the eCPRI open interface between the RU and DU.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 196, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0b00bf9fa47b202d3ebb691eb57aca18', 'text': 'Figure 4-25 illustrates the evolution of the SecGW to secure the distributed RAN deployments in the O-RAN architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 196, 'parent\_id': 'f696a07d51e4fe9e07a0daf910ccc524', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '58ef4617d6ef1c030e483e6698db9cec', 'text': 'Open front Haul —> 5G SA ((A)) = (C-RAN/O-RAN/VRAN) Xn i Xn, N2, N3 oo A ‘\_ Xn - o o e 5G NSA (A) Xx, Xn, N2, N3 N2, N4 i 50CP S6UP : S1, X2, Sx §1,X2 4G CUPS ((A)) e 0 = eue seup ~ - Centralized 5GC = o and EPC - MEC " ((A) L She', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 197, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '77c8e81528987c79b93eabe27232284e', 'text': 'Figure 4-25 Evolution of SecGW Architecture to Secure 5G C-RAN/O- RAN/VRAN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 197, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e929700361571e53eb5ff03ab4667643', 'text': 'Figure 4-26 provides an example of securing the O-RAN deployment using the SecGW.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 197, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '271a1e3e5f6f4e9574b9ca7b6738377d', 'text': 'AAU ( e N2 N2, N4 F1 FH | F1 .H R S N3 Far Edge DC Central DC = A \_\_ Edge DC N6', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 198, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '063f4066245b89a8b9efb0eab4263a5d', 'text': 'Figure 4-26 SecGW Deployment Specific to Secure O-RAN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 198, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '21e23c1d23c9497bac7ece0851ee8c6a', 'text': 'As you can see from Figure 4-26, both the centralized and distributed SecGW deployment modes are used to secure the 5G O-RAN deployment. Normally the CU-UP and the UPF are deployed in the same rack and are within a trusted zone. But if the CU-UP and the UPF are in separate locations, then the N3 interface needs to be secured using the SecGW.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 198, 'parent\_id': '063f4066245b89a8b9efb0eab4263a5d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ba0462dd37bb37f27c72865f7ec0ad26', 'text': 'Securing the F1 Interface', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 198, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5a25b8d50a86758e6297c5ef55ccaa51', 'text': 'The interface between the gNB-DU and the gNB-CU is called the F1 interface. The F1 interface consists of the F1-C interface and the F1-U interface. F1-C is the interface between the gNB-CU-CP and gNB-DU-CP interface. F1-U is the interface between the gNB-CU-UP and gNB-DU-UP interface. Figure 4-27 illustrates the deployment of SecGW in the location of the CU to aggregate multiple DUs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 198, 'parent\_id': 'ba0462dd37bb37f27c72865f7ec0ad26', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'eebb9fda23e6423be0fbfd9721616838', 'text': 'IPsec tunnel mode F1-U B N3 Edge DC ;', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 199, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bc3c2033e4c3c58a55547bafe396d691', 'text': 'Figure 4-27 SecGW at CU Location Aggregating IPsec from Multiple DUs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 199, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '15f33d64d6812590dfe494953bcd87ac', 'text': 'Usually, the gNB-CU is deployed in the topology as an aggregator of gNB- DUs. The number of gNB-DUs supported by gNB-CU is dependent on a number of factors, but primarily its attributed to the max CPU allocated to the virtual instance of CU and the CPU consumed per virtual instance of DU. The F1-C interface gNB-DU-CP and gNB-CU-CP usually has IPsec tunnel support built in.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 199, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '414904eee90657a11a3119c329b6a8b4', 'text': 'F1-U has a mandatory requirement for IPsec support, and the deployment of cryptographic solutions like SecGW is purely the choice of the service provider. The gNB-CU-UP scales in and out depending on traffic. Correspondingly, F1-U EPs (endpoints) are added and removed dynamically, and any gNB-DU can interface with any gNB-CU-UP F1-U EP for a given UE session. This makes the implementation of IPsec with mapping per gNB-DU- UP and gNB-CU-UP impractical because it needs the service provider OAM to configure the IPsec tunnel between the gNB-CU-UP and gNB-DU-UP pair.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 199, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a12823a50bacbedb6b7bf09879b05243', 'text': 'The recommended way to deploy cryptographic solutions like SecGW to provide ESP and IKEv2 certificate-based security in the F1-U interface is to have a SecGW deployed at the DC, as shown in the preceding figure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 199, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a30f64c720f69c82bc5a98876226761e', 'text': 'Table 4-5 outlines the security control for C-RAN/O-RAN/VRAN deployment. Please note that the RAN components, such as CU and DU, are all O-RAN compliant and that the naming convention is kept as gNB-CU instead of O-CU to be consistent across O-RAN, C-RAN, and VRAN architectures.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 200, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '4fceb550d8b769a518ecffd59714724b', 'text': 'Interface Access Node / O- Core Node Recommended RAN Node Security Control OAM N2 N3 Xn-C Xn-U El F1-C F1-U 0] Service Management and Orchestration <> gNB-CU-CP gNB-CU-UP gNB-DU-CP gNB-DU-UP Al L R', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Interface</th><th>Access Node / O- RAN Node</th><th>Core Node</th><th>Recommended Security Control</th></tr></thead><tbody><tr><td>0AM</td><td></td><td></td><td></td></tr><tr><td>N2</td><td></td><td></td><td></td></tr><tr><td>N3</td><td></td><td></td><td></td></tr><tr><td>Xn-C</td><td></td><td></td><td></td></tr><tr><td>Xn-U</td><td></td><td></td><td></td></tr><tr><td>El</td><td></td><td></td><td></td></tr><tr><td>F1-C</td><td></td><td></td><td></td></tr><tr><td>F1-U</td><td></td><td></td><td></td></tr><tr><td>0l</td><td>Service Management and Orchestration &lt;&gt; gNB-CU-CP gNB-CU-UP, gNB-DU-CP, gNB-DU-UP</td><td></td><td></td></tr><tr><td>Al</td><td>peowe</td><td></td><td>™</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 200, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '50565e88fb14eabdbae5de4046d302f1', 'text': 'Open FH M- gNB-DU<>RU | NETCONF/TLS plane with PKIX for certificate-based mutual authentication and SSHv2 with RFC 6187 support for PKIX-based SSHv2. Open FH CUS- gNB-DU<>RU | 802.1X and plane MACsec. (O-RAN is discussing the use of 1588-2019 with the newly defined security TLV to protect announce messages.) E2 RIC <> third- X-r Apps RBAC, party applications Segmentation, API protected by TLS.', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Open FH M- plane</th><th>gNB-DU&lt;&gt;RU</th><th>|</th><th>NETCONF/TLS with PKIX for certificate-based mutual authentication and SSHv2 with RFC 6187 support for PKIX-based SSHv2.</th></tr></thead><tbody><tr><td>Open FH CUS- plane</td><td>gNB-DU&lt;&gt;RU</td><td>|</td><td>802.1X and MACsec. (O-RAN is discussing the use of 1588-2019 with the newly defined security TLV to protect announce messages.)</td></tr><tr><td>E2</td><td></td><td></td><td></td></tr><tr><td>X-r Apps</td><td>RIC &lt;&gt; third- party applications</td><td></td><td>RBAC, Segmentation, API protected by TLS.</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 201, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f6e18089d45677224a57b9f8b3c2286e', 'text': 'Table 4-5 Security Controls per Interface O-RAN/C-RAN/VRAN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 201, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '637de275c313e99f441864b1f0028c2b', 'text': 'Table 4-6 outlines the security controls for multi-RAT deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 201, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '3c310339cce00ab36b3adffea50abbcb', 'text': 'Interface Access Node Core Node Recommended Security Control OAM X2-C X2-U S1-C S1-U SGW-U IPsec Sxa SGW-U <> SGW-C [Psec Sxb = Sxc TDF-U <> TDF-C IPsec Xn-C [Psec Xn-U IPsec N2 AMF [Psec N3 [Psec N4 = N2 N3 eNB-CU-UP [Psec Xn-C gNB-CU-CP [Psec Xn-U IPsec eNB-CU-UP El gNB-CU-CP <> [Psec eNB-CU-UP F1-C F1-U', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Interface</th><th>Access Node</th><th>Core Node</th><th>Recommended Security Control</th></tr></thead><tbody><tr><td>OAM</td><td></td><td></td><td></td></tr><tr><td>X2-C</td><td></td><td></td><td></td></tr><tr><td>X2-U</td><td></td><td></td><td></td></tr><tr><td>S1-C</td><td>R</td><td>L L</td><td></td></tr><tr><td>S1-U</td><td>eNB</td><td>SGW-U</td><td>IPsec</td></tr><tr><td>Sxa</td><td></td><td>SGW-U &lt;&gt; SGW-C</td><td>[Psec</td></tr><tr><td>Sxb</td><td></td><td></td><td></td></tr><tr><td>Sxc</td><td></td><td>TDF-U &lt;&gt; TDF-C</td><td>IPsec</td></tr><tr><td>Xn-C</td><td>gNB-¢g gNB</td><td></td><td>[Psec</td></tr><tr><td>Xn-U</td><td></td><td></td><td>IPsec</td></tr><tr><td>N2</td><td>gNB</td><td>AMF</td><td>[Psec</td></tr><tr><td>N3</td><td>gNB</td><td></td><td>[Psec</td></tr><tr><td>N4</td><td></td><td>L</td><td></td></tr><tr><td>N2</td><td></td><td></td><td></td></tr><tr><td>N3</td><td>eNB-CU-UP</td><td></td><td>[Psec</td></tr><tr><td>Xn-C</td><td>gNB-CU-CP</td><td></td><td>[Psec</td></tr><tr><td>Xn-U</td><td>eNB-CU-UP</td><td></td><td>IPsec</td></tr><tr><td>El</td><td>gNB-CU-CP &lt;&gt; eNB-CU-UP</td><td></td><td>[Psec</td></tr><tr><td>F1-C</td><td></td><td></td><td></td></tr><tr><td>F1-U</td><td></td><td></td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 202, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cb69648b29e75de66120bc06d7c40ab3', 'text': 'Table 4-6 Security Controls from 4G Toward 5G O-RAN/C-RAN/VRAN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 203, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3b7f2e4600cd74820221dd10890c22c9', 'text': 'DDoS Protection', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 203, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '368a27bce7a528bb8cc43f32ced5ec16', 'text': 'Evolving the back-haul and RAN architectures necessitates enhanced transport security, which includes DDoS security to cater for interface protection between multi-RAT communications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 203, 'parent\_id': '3b7f2e4600cd74820221dd10890c22c9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '837df2c9e7bfe9cd71a894d3738fef62', 'text': 'There are three primary types of DDoS attacks:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 203, 'parent\_id': '3b7f2e4600cd74820221dd10890c22c9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '914d07847a99c39fb328daa52e8196bb', 'text': '• Volume-based attacks: Some examples of volume-based DDoS attacks follow:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 203, 'parent\_id': '3b7f2e4600cd74820221dd10890c22c9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a19a6e8f0e907cbfc99cdcfd5f1b2172', 'text': '• UDP flood example: A User Datagram Protocol (UDP) flood targets random ports on a remote server with requests called UDP packets. The host checks the ports for the appropriate applications. When no application can be found, the system responds to every request with a “destination unreachable” packet. The resulting traffic can overwhelm the service.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 203, 'parent\_id': '3b7f2e4600cd74820221dd10890c22c9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d4d58a44d6839a77bd14cc47ddc9b8d', 'text': '• ICMP (ping) flood example: An Internet Control Message Protocol (ICMP) flood sends ICMP echo request packets (pings) to a host. Pings are common requests used to measure the connectivity of two servers. When a ping is sent, the server quickly responds. In a ping flood, however, an attacker uses an extensive series of pings to exhaust the incoming and outgoing bandwidth of the targeted server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 203, 'parent\_id': '3b7f2e4600cd74820221dd10890c22c9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '63506420ab41497c94e713a6c520f7d4', 'text': '• Application attacks: Some examples of application-based DDoS attacks follow:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 203, 'parent\_id': '3b7f2e4600cd74820221dd10890c22c9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '14f1e7f9fd0bf80a4c1213a71389194b', 'text': '• HTTP flood example: An HTTP flood is a Layer 7 application attack that uses botnets, often referred to as a “zombie army.” In this type of attack, standard GET and POST requests flood a web server or application. The server is inundated with requests and may shut down. These attacks can be particularly difficult to detect because they appear as perfectly valid traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 203, 'parent\_id': '3b7f2e4600cd74820221dd10890c22c9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fa85b3d661aeb95967a33b5382b441a3', 'text': '• Slowloris example: Named after the Asian primate, the Slowloris attack moves slowly. It sends small portions of an HTTP request to a server. These portions are sent at timed intervals, so the request does not time out, and the server waits for it to be completed. These unfinished requests exhaust server resources such a memory and affect the server’s ability to handle legitimate requests.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 203, 'parent\_id': '3b7f2e4600cd74820221dd10890c22c9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '011da2076ac530af4df1c626d9f5f7bf', 'text': '• Protocol attacks: Some examples of protocol-based DDoS attacks follow:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 204, 'parent\_id': '3b7f2e4600cd74820221dd10890c22c9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '92dba81ca4def15d2ca42b8558b366cd', 'text': '• SYN flood example: In a SYN flood attack, the attacker sends seemingly normal SYN requests to a server, which responds with a SYN-ACK (synchronized-acknowledgment) request. Typically, a client then sends back an ACK request, and a connection is made. In a SYN flood attack, the attacker does not respond with a final ACK. The server is left with a large number of unfinished SYN-ACK requests that burden the system.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 204, 'parent\_id': '3b7f2e4600cd74820221dd10890c22c9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '76ce68025feb075cad7d8e8265efd9eb', 'text': '• Ping of Death example: In a Ping of Death attack, the attacker tries to crash or freeze a server by sending a normal ping request that is either fragmented or oversized. The standard size of an IPv4 header is 65,535 bytes. When a larger ping is sent, the targeted server will fragment the file. Later, when the server formulates a response, the reassembly of this larger file can cause a buffer overload, resulting in a crash.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 204, 'parent\_id': '3b7f2e4600cd74820221dd10890c22c9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '98ccf8c61397a69b4be07ebc6f18311c', 'text': 'The transport layer of the 5G network is more susceptible to volume-based attacks and protocol attacks. With 5G having customer premises equipment (CPE) with capacity of 1Gbps, a huge DDoS attack could occur if the CPE becomes the victim of a malicious actor who then attacks the network infrastructure, forcing the content servers, which are susceptible to high- volume and protocol attacks from CPE, to crash. The high traffic coming from the CPE also consumes the bandwidth of the back haul, thereby reducing the bandwidth available to the legitimate traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 204, 'parent\_id': '3b7f2e4600cd74820221dd10890c22c9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '74c44cf30811e6ac9395f6b6220569d3', 'text': 'DDoS protection/anti-DDoS mechanisms are usually deployed at the Internet peering or Gi/N6 interface, as illustrated in Figure 4-28. This deployment would help you secure your network from inbound DDoS attacks from the Internet.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 204, 'parent\_id': '3b7f2e4600cd74820221dd10890c22c9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '95772c547116f2df0279beb56f5c1cd6', 'text': 'Usual location for deployment of Anti-DDoS mechanism A) ->\_<->E-< -<—> Front Haul / MEC Back Haul Mid Haul Centrahzed packet core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 205, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f6cbde7723662165d3b4d734418e4519', 'text': 'Figure 4-28 Typical Location of DDoS Protection Solution', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 205, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f013e030df6515ded23c0715a7ddd3d5', 'text': 'One way to mitigate the DDoS threats from the CPE toward the content servers and inbound from the Internet, both at the edge and central DC layers, is to have anti-DDoS solutions deployed both at the MEC and central DC layer to protect the back haul, as illustrated in Figure 4-29.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 205, 'parent\_id': 'f6cbde7723662165d3b4d734418e4519', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a326024fd79c8ad777679ab56b2c286d', 'text': 'Central analysis & decision making Distributed enhanced Anti-DDoS flow monitors + mitigation action (containers or appliances) ™ -g- [0 — | == B« == A« >IEEE «— A gNB Front Haul / MEC Back Ha Mid Haul Centralized packet core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 205, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c4247f52fd2505b4ece2123ce55eaa56', 'text': 'Figure 4-29 Distributed DDoS Protection Solution', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 205, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8a1f57574baf902122905e2f92ca5839', 'text': 'For 5G-related DDoS attacks from various types of IoT devices (consumer, industrial, and so on), it is important that the service providers choose a DDoS solution that not only can mitigate the threats from the edge of the network but', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 205, 'parent\_id': 'c4247f52fd2505b4ece2123ce55eaa56', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cebf42423b8425c1d97d1519adc1c18e', 'text': 'also have high accuracy of detection and mitigation as well as strong automation to ensure multivector mitigation actions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 206, 'parent\_id': 'c4247f52fd2505b4ece2123ce55eaa56', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'de6f02a15e895118243bde362fd6a585', 'text': 'Attacks are becoming completely automated and more sophisticated, making it difficult to defend against them manually. New techniques like burst attacks and advanced persistent denial of service (APDoS) demand advanced detection and mitigation and underscore the need for automation. Automation is at the core of a successful DDoS attack mitigation solution. To withstand the evolving threat landscape, service providers need to have anti-DDoS solutions with enhanced algorithms in place to shorten the response time and automatically respond to attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 206, 'parent\_id': 'c4247f52fd2505b4ece2123ce55eaa56', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '549b0185454d4916004291caa002cb25', 'text': 'With continuous monitoring and intelligence, service providers can detect a wide range of attacks before they wreak havoc on the network. These attacks/symptoms include the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 206, 'parent\_id': 'c4247f52fd2505b4ece2123ce55eaa56', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ffa9606f24d1f670c6c371fd47a0e12f', 'text': '• Behaviors related to zero-day malware', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 206, 'parent\_id': 'c4247f52fd2505b4ece2123ce55eaa56', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd42afa14e0d3fc47d3d3ba466d8bb269', 'text': '• Insider threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 206, 'parent\_id': 'c4247f52fd2505b4ece2123ce55eaa56', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '03af8dfc2dfd559d696c5b6c41c848d6', 'text': '• Advanced persistent threats (APTs)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 206, 'parent\_id': 'c4247f52fd2505b4ece2123ce55eaa56', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4535db6e9c4021a865f8cafb5199af92', 'text': '• Distributed denial-of-service (DDoS) attempts', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 206, 'parent\_id': 'c4247f52fd2505b4ece2123ce55eaa56', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '66cec1467c3e664d817c5d1b71ac226a', 'text': 'To enable detection of such malicious traffic, monitoring is required, not only on the traffic going in and out of the network but also on the lateral (east-west) traffic inside the network to identify network abuse and insider threats. Traditionally, known insider attacks are perpetrated on the network by individuals working for the organization. In 5G deployments, insider threats extend to IoT devices and industrial IoT devices (IIoT) that are deployed as a part of the Non-Public Network (NPN) or Public Network Integrated Non- Public Network (PNI-NPN), such as critical infrastructure verticals. These IoT/IIoT devices are authenticated to the network using 5G authentication mechanisms and are seen as part of the trusted network within a network slice, such as an IoT slice. Even if one of these devices or the network gateway controlling the devices is upgraded with an exploited patch that includes modified malicious code, the entire IoT/IIoT slice can cause forced paging, thereby consuming the resources and preventing legitimate devices from accessing the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 206, 'parent\_id': 'c4247f52fd2505b4ece2123ce55eaa56', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6f4a53e565a588b2bfa4e38b22b560ee', 'text': 'Using the continuous monitoring method, an anomaly in the network traffic in the front haul, mid haul, back haul, or Internet peering can be detected. Once the anomaly is detected, the information can be sent to the central analysis and', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 206, 'parent\_id': 'c4247f52fd2505b4ece2123ce55eaa56', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0f3f23a56f80388b89be985345fc798f', 'text': 'decision-making center, which can take a deeper look at the anomaly and, depending on the analysis, can command the distributed anti-DDoS devices to control the flow of the anomalous traffic. These distributed anti-DDoS devices, which are deployed at the edge of the network (such as the transport and MEC layer) are also referred to as distributed flow controllers, as their main function is to control the flow of the data traffic across the switches and routers in the transport and MEC layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 207, 'parent\_id': 'c4247f52fd2505b4ece2123ce55eaa56', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2555569f1cd994c6cfe6335150c6c926', 'text': 'For mitigating DDoS attacks based in UDP flood, you should use the anomaly detection solution, which detects any behavioral anomaly within your network, to identify the large number of inbound UDP packets on irregular ports and then decide the mitigation methods such as dropping/logging the packets automatically before the attack impacts the servers. This is not required if DDoS protection solutions are deployed in your network. The DDoS solution would automatically identity and mitigate DDoS attacks such as UDP flood attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 207, 'parent\_id': 'c4247f52fd2505b4ece2123ce55eaa56', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '837779f0eddc37e1e763afad7f45b413', 'text': 'Real Scenario Case Study: Examples of Threat Surfaces and Their Mitigation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 207, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9697cb2da9fb40a869f3135214fa55aa', 'text': 'This section of the chapter takes you through some real scenarios seen in labs, proof-of-value deployments, and attacks seen in networks very similar to 5G deployments. At press time, 5G is still being deployed, and most of the networks are in nascent stages. Having this real-world view might provide you with that extra edge in understanding the exact threat vector so you can make the necessary reviews of the design you plan to deploy and then make the necessary enhancements to the security architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 207, 'parent\_id': '837779f0eddc37e1e763afad7f45b413', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c176b7bda6fba66070c28edbf9a1e989', 'text': 'Figure 4-30 shows three primary threat vectors:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 207, 'parent\_id': '837779f0eddc37e1e763afad7f45b413', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3dcce18ee92fc5539a4bd4e91c191fa5', 'text': '• A: The attacker takes control of IoT devices with weak security and launches a DDoS attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 207, 'parent\_id': '837779f0eddc37e1e763afad7f45b413', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '39e77340d4012516af8c8a6d367f9243', 'text': '• B: The attacker uses the vulnerability in insecure transport to use rogue eNBs/fake base stations and uses attacks such as MitM in the 5G deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 207, 'parent\_id': '837779f0eddc37e1e763afad7f45b413', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '31e32c63954781e26593f9f0e505e8ec', 'text': '• C: The attacker uses the insecure transport and carries out MitM attacks in back haul.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 207, 'parent\_id': '837779f0eddc37e1e763afad7f45b413', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '8bac16e91654ca4b0d8218664335c2ae', 'text': '® o N Attacker | , S~ Vep (R 0 N \\ ~ Internet \\ AK— L/ = R < gNB \_d — MEC Centralized 4G & 5G o Packet Core =g W@ eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 208, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '576de541e23866709104f2561782c7d5', 'text': 'Figure 4-30 Example of Threat Vectors', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 208, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eb18bf5fb9824d9ea20758555e1cd45e', 'text': 'The sections that follow analyze the threat vectors (A, B, and C) in more detail.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 208, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'fb30973987795bceb9d96681f5bef07f', 'text': 'A: The Attacker Takes Control of IoT Devices with Weak Security and Launches DDoS Attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 208, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '912d9a4dd3c82ec589777503efa6d676', 'text': 'DDoS attacks can be from subscriber 5G IoT terminals that are being served by the service provider, or they can be from external bots from the Internet trying to take down the service provider network infrastructure such as the DNS servers (also called inbound attacks), as illustrated in Figure 4-31.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 208, 'parent\_id': 'fb30973987795bceb9d96681f5bef07f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '63d505924e7fd144417e5b3486f7e05c', 'text': 'Inbound DDoS attacks from Internet towards the service provider networks DDoS attacks from internal network (loT devices being served by service provider) - ( A)) d » ONB < 4 MEC Centralized 4G &5G SR Packet Core - w=— eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 209, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d7223e1f75f14a5d6fa930efd29259b', 'text': 'Figure 4-31 Internal Devices and Inbound DDoS Attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 209, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f2e36d371f5ec2d4e07a09f8fe15f2a3', 'text': 'Figure 4-31 shows the two key DDoS threat vectors: inbound DDoS attacks and DDoS attacks from internal DDoS devices served by the 3GPP and non- 3GPP technologies served by the service provider.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 209, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aecd8d4e8666c42bf44cb462ede3a70a', 'text': 'There are many variants of the inbound DDoS attacks. The UDP flood attack is one of them, where the attacker uses a botnet to send large amounts of traffic to the service provider’s server, which could be a server deployed in the public or telco cloud infrastructure serving the subscribers with a specific application. UDP attacks are generally very rapid in nature, and the aim of such attacks is primarily to consume the available bandwidth allocated to the server rather than to exhaust server resources, which allows the attacker to prevent the bandwidth being allocated to the legitimate user. Successful UDP attacks usually follow a trend where a large number of packets arrive, each with different destination ports, and the server is forced to process each of the packets and also respond to each of the requests. The servers in such attacks could be taken down very fast, sometimes in minutes, leaving very little time for incident response teams to react to such attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 209, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9b2fcce9605b3d00a26be63a19dc45ad', 'text': 'B: The Attacker Uses the Vulnerability in S1 and Insecure Transport to Use Rogue eNBs and Uses', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 209, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1afdc1037ab6d743e5e4e727865c94ca', 'text': 'MitM Attacks in the 5G NSA Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 210, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6bc5f233286f816dbf1816ade1b209c5', 'text': 'The capabilities of rogue/false base stations vary depending on whether the mobile network is GPRS, UMTS, LTE, or 5G. The 5G system in particular has already made significant improvements to combat false base stations, but as mentioned earlier in this section, there are still facets of this threat vector that need further validation to understand the new protection mechanisms and detect vulnerabilities within the new authentication mechanisms in 5G. Early 5G commercial networks are being deployed using 3GPP’s NSA 5G specifications, meaning these networks are required to use the LTE control plane protocols and the LTE Evolved Packet Core network. 5G NSA networks based on LTE core networks have been deployed in many service providers and will continue to operate in the networks for more years, so any LTE threats and vulnerabilities will also exist in the 5G NSA network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 210, 'parent\_id': '1afdc1037ab6d743e5e4e727865c94ca', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '14cfab6187c10a68989f16e80f2180fc', 'text': 'In Figure 4-30, the attacker exploits the vulnerabilities in the LTE S1 interface and the vulnerabilities in the insecure and untrusted transport network to attack the service provider’s infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 210, 'parent\_id': '1afdc1037ab6d743e5e4e727865c94ca', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'fe5562251dcd4b6b96cab3727ebb876b', 'text': 'C: The Attacker Uses the Insecure Transport and Carries Out MitM Attacks in Back Haul', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 210, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '280a9bbb09e8e7a87bf0829e2fb112cc', 'text': 'In Figures 4-30 and 4-31, the attacker uses the insecure hardware and software within the transport network elements, such as a pre-aggregation or an aggregation router, leading to threats based on MitM threat vectors such as sniffing, data exfiltration, and modifying the packets in the transport. The programmable transport network devices also support API for integration with the SDN controllers and fabric layers. If the API is insecure, the attacker could use the API capability of the transport network element to make modifications to the configuration and cause it to drop traffic, leading to DoS or network outage. The attacker could also use the API to take the configuration dump, which might have information such as the IP address of other network elements. This can then be taken under control by the attacker.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 210, 'parent\_id': 'fe5562251dcd4b6b96cab3727ebb876b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5ed0c59b33b2b11b45aff92790881b24', 'text': 'Mitigation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 210, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3bda56af2f6e4d28ce66d24d20d37f24', 'text': 'This section takes you through the security controls to mitigate the threats shown in Figures 4-30 and 4-31.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 210, 'parent\_id': '5ed0c59b33b2b11b45aff92790881b24', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8383f2b97d9a5a2b16a0924f071fc8d3', 'text': 'Detection of Rogue Base Stations and False Base Stations', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 211, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '346f6adedea7baee1af31980a3198439', 'text': 'Figure 4-32 illustrates one of the mechanisms to detect the rogue/fake 4G or 5G base stations (eNB/gNB). This mechanism uses the key performance indicators (KPIs) calculated using the UE measurements. The UE would normally provide the received signal strength and quality, along with the location information, in measurement reports. These measurement reports are normally used by various tools, such as the RAN vendor’s performance reporting solution, radio optimization tools, or self-organizing network (SON) solutions, to optimize the network, such as improving intra-RAT/inter-RAT handovers, reducing dropped call rates, improving signal quality by antenna down tilt and azimuth correction, and so on, thereby improving the subscriber experience.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 211, 'parent\_id': '8383f2b97d9a5a2b16a0924f071fc8d3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5f26d863f9bde39483bcaec8f83b3aef', 'text': 'o o Attacker l Rogue/fake Data snooping, SUCI A) eNB or gNB collection for replay controller attacks, etc Rogue/fake gNB, eNB (( UE KPI gNB < Rogue/fake Identification of T RAN 0SS & Measurements gNB or eNB EMS detector Rogue/fake eNB or gNB Air mlerface measurements by UE eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 211, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7898c284c54392d17f04689511e5f3d6', 'text': 'Figure 4-32 Detection of Rogue/Fake Base Stations', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 211, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4e1e98523dc623899af98cf4debd14f7', 'text': 'These UE measurements can also be put to use to detect any rogue or fake base stations. Some methods are explained in the list that follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 211, 'parent\_id': '7898c284c54392d17f04689511e5f3d6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d5695b68629ad3fafce880d037e94e9', 'text': '• One example of detection could be because of random spikes in interference, specifically uplink (UL) interference. UL interference could be due to various reasons, including faulty repeaters or a high Voltage', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 211, 'parent\_id': '7898c284c54392d17f04689511e5f3d6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bcc9f6a332b022f75b34ed0ba36e7773', 'text': 'Standing Wave Ratio (VSWR) in legacy deployments. Rogue/fake base stations also cause high UL interference due to operating on the same frequency channel as the legitimate base station. Depending on the RAN vendor being used by the service provider, a customer KPI showing UL interference in a cluster or a KPI on the cell level would help to narrow down the possibility of a rogue/fake base station.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 212, 'parent\_id': '7898c284c54392d17f04689511e5f3d6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '968f927276c1c6e9fd7d1f1cf65b8b87', 'text': '• Another method is to use the UE measurements to identity base stations (eNB/gNB) that are transmitting at an incorrect frequency or a higher power using the service provider’s PLMN (public land mobile network). This could be due to unintentional misconfiguration or could be a rogue/fake base station trying to pump more power and forcing the UE in a specific location to select or hand over to the rogue/fake base station.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 212, 'parent\_id': '7898c284c54392d17f04689511e5f3d6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1fbd11df40772b25597acebfd3124347', 'text': 'Once the cluster or approximate location is known, a spectrum analyzer can pinpoint the location of the suspected base station.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 212, 'parent\_id': '7898c284c54392d17f04689511e5f3d6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4d44e346779d6a1144443ae716ff8fc6', 'text': 'Deploy Trusted Hardware and Software', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 212, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b2eaf578f9b27cf60c453ed77c0d3e34', 'text': 'Service providers who plan to deploy programmable transport network elements for the 5G network rollout should ensure that the transport vendors being chosen to follow an internal secure development lifecycle, including software (including API) and hardware hardening to mitigate any possibility of attackers trying to take control of the programmable network elements. Figure 4-33 illustrates how trusted hardware and software along with SZTP implementation protects your transport deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 212, 'parent\_id': '4d44e346779d6a1144443ae716ff8fc6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '07a80e9fdb14e3a01bbdd8b7d3ba9791', 'text': '~ Y Y Secure access between PnP / provisioning server and transport network device a T — Attack A e Fa e e gNB 4+— " 4 T« o . S = CEEe Trusted HW & sw ) Centalized | ME‘ - 4G &5G e K Packet Core - —-——— Trusted HW & SW ) eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 213, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4e17e2e6220163da3332def016282ec6', 'text': 'Figure 4-33 Secure ZTP and Trusted HW and SW', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 213, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ccf83d9a0d0c4ea947c80d1766348a7c', 'text': 'A majority of transport solution vendors today support different variants of ZTP and API interfaces to allow seamless integration with the SDN network and to allow easier deployment and provide regular updates of transport layer network elements.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 213, 'parent\_id': '4e17e2e6220163da3332def016282ec6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6c651fff4f8988b887051e383a1b77d1', 'text': 'Following the SZTP process during pre-deployment, deployment, and operation explained in detail earlier in this section, service providers would mitigate the threat vector of attacks from attackers trying to exploit vulnerabilities in the transport access devices. If the service provider overlooks security controls like using trusted hardware and software, secure SZTP servers, and secure communication between the transport access device and SZTP servers, it would be very difficult to contain the rising threat vectors.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 213, 'parent\_id': '4e17e2e6220163da3332def016282ec6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ec20afb17dd58f63738998b9d6d37f2b', 'text': 'In other words, it is imperative that the security controls discussed are deployed by the service providers planning to deploy new transport access devices for 5G. If there are existing transport access devices that do not have trusted components or use a secured bootstrap or provisioning servers, it’s recommended not to use them for 5G deployments or integration with the SDN controller used for 5G network slicing.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 213, 'parent\_id': '4e17e2e6220163da3332def016282ec6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3230fb571414080702c7f73ba86020f8', 'text': 'Before selecting the 5G equipment vendor, it is very important that you check whether the vendor provides you with the mechanism to ensure that you can verify the integrity of the hardware and software being deployed. One of the mechanisms would be a management layer of the solution that shows you if the secure booting process is successful and maintains a list of the upgrade and patch history for the equipment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 214, 'parent\_id': '4e17e2e6220163da3332def016282ec6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '35bce4e1dd6d1c427d180c1e945f0327', 'text': 'Granular Access Control', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 214, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8765913c608d4a3a7005d76d092e62c7', 'text': 'Apart from the access control for the RAN and transport elements, service providers must also ensure that the RAN and transport devices support role- based access control (RBAC) and that granular policies can be applied to the RAN and transport network elements. The RBAC controls should be further integrated with multifactor authentication (MFA) solutions to provide granular user and device policy enforcement. Having this layer of protection will provide granular mapping between the vendors and the configuration engineers, thereby only allowing configuration engineers of specific vendors access to their equipment. One way the access controls can be implemented is by using a global Identity and Access Management (IAM) solution integrated with a global policy engine where you can configure the user policies. The IAM solution should then be integrated with an MFA solution to ensure that each and every user goes through the secondary authentication mechanism to provide an added layer of access security. The RAN disaggregation into Distributed Unit (DU) and Centralized Unit (CU) requires a deeper look into the dynamic capabilities of deployment, which will require integration with the orchestration and automation layer. Orchestration and automation, though relevant in 4G, are more relevant in 5G due to the disaggregation and virtualization of the 5G network functions. The security controls around virtualization are better explained in the chapters “Securing MEC Deployments in 5G” and “Securing Virtualized 5G Core Deployments”. Orchestration is very important for the 5G-related transport access network due to the closer integration required with the SDN fabric for network slicing. Here is where proper strategy needs to be made around orchestration capabilities and dependencies around the transport network access devices. Due to the relevance of orchestration in the RAN and transport layer, the access control on the orchestration should be applied at a granular level. Figure 4-34 illustrates the granular control required, which should cater to different parts of the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 214, 'parent\_id': '35bce4e1dd6d1c427d180c1e945f0327', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'aec9d7b8cf490f8958dbb07802344ed8', 'text': 'v Granular Access control Al 4 oy £ e Ry ((A)) 4 MEC Centralized 4G &5G ————— Packet Core T — ((A)) eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 215, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '82d2102e0f4a980adc913a4837dd0f81', 'text': 'Figure 4-34 Granular Access Control', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 215, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'bb30d9a250ff1fb875782e2a5e26425c', 'text': 'Security Gateway', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 215, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5041922b200da5c053553b75b2cc13e7', 'text': 'The topic of rogue/fake 4G and 5G RAN nodes has been discussed in detail in earlier sections. A security gateway uses digital certificates provided by the service provider’s PKI infrastructure for authentication. Figure 4-35 illustrates the mitigation of fake/rogue gNB/eNB attacks by using a SecGW.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 215, 'parent\_id': 'bb30d9a250ff1fb875782e2a5e26425c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '8cafa18a6ecd1f9b06ba5e8c411da5ec', 'text': 'Rogue gNB / eNB((A)) -——— - P T g v \_d g\\B K E - [ e - ——— (x) MEC Centralized 4G & 5G Packet Core eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 215, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '11f014c9296cdc4e3a5a7af28d149694', 'text': 'Figure 4-35 Security Gateway Mitigating Rogue/Fake RAN Nodes', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 216, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cd94e3f2016ace04ef6b73aaaf7c12b8', 'text': 'SecGW deployment between the radio access nodes (eNB, gNB, pico cells, small cells, and so on) and the mobile packet core provides both authentication and encryption. 3GPP has specified mandatory support of the IPsec stack for 4G and 5G radio access nodes, which means you would be required to deploy SecGW only at the mobile packet core location. SecGW is not required at the radio access node location, as the IPsec stack within the radio access node will perform the IPsec tunnel initiation and termination to and from the SecGW.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 216, 'parent\_id': '11f014c9296cdc4e3a5a7af28d149694', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e4484275badeea57d336a6c2d2ff54bd', 'text': 'The radio nodes (eNB/gNB) are pre-provisioned with a public-private key pair by the RAN vendor and have the vendor-signed certificate of their public key pre-installed. Public key infrastructure (PKI) is used to deploy a service provider–signed certificate within the radio node and the service provider–root certificate within the SecGW. The service provider normally uses an RA/CA, which can be a standalone CA with Certificate Management Protocol version 2 (CMPv2). A key point here for you to check is the support of CMPv2 protocols by the SecGW vendor. The CMPv2 protocol, based on RFC 4210, is a PKI protocol for managing X.509 certificates. CMPv2 is used between Certification Authorities (CAs), Registration Authorities (RAs), and end entities (EEs). In CMPv2, most communication is initiated by the EEs, where every CMP request triggers a CMP response message from the CA or RA. This provides a means for initial registration of end entities, key pair update and certificate updates for end entities and CAs, cross-certification between CAs, certificate revocation management, and discovery of certificates and certificate revocation lists (CRLs). CMPv2 provides better lifecycle management of the SecGW by providing functionalities such as certificate revocation and re-enrollment of certificates. For example, if any of the RAN nodes is found to be exploited, the certificate of all RAN nodes can be revoked, and new certificates can be enrolled by using CMPv2 to prevent the attackers getting access to the network using the previously exploited certificate.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 216, 'parent\_id': '11f014c9296cdc4e3a5a7af28d149694', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '47a7836515c3d20afa4cb963da6b1f97', 'text': 'The mutual authentication process is carried out between the radio nodes and the SecGW using the X.509 certificates during the IPsec tunnel setup process. In the mutual authentication process, the radio nodes will validate the certificate of the SecGW to ensure that it is connecting to the right network. The SecGW also validates the certificate of the radio node to verify its identity. Once the SecGW and the access nodes are authenticated, they will treat each other as trusted nodes and will establish an IPsec tunnel between them and provide encryption to the traffic between the radio access nodes and the mobile', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 216, 'parent\_id': '11f014c9296cdc4e3a5a7af28d149694', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7d7cb818c04513bad122bc7e6340ac98', 'text': 'packet core network. This process of mutual authentication cannot be passed by the rogue access nodes, as it does not have the certificates deployed in the legitimate access nodes by your PKI infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 217, 'parent\_id': '11f014c9296cdc4e3a5a7af28d149694', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5b83290173c0cc660e56f751c3f2ce6c', 'text': 'IKE, ESP, and AH security associations use secret keys to encrypt the data traffic for a finite period, which limits the entire security association (SA). To ensure interruption-free traffic, a procedure called rekeying is used, where a new SA takes the place of the expiring SA. This rekeying procedure also makes it much harder for the attacker to derive the secret keys used to encrypt the traffic between radio access nodes and the SecGW.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 217, 'parent\_id': '11f014c9296cdc4e3a5a7af28d149694', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7e4a1ded5190c650f697ba0a374ff839', 'text': 'DDoS Protection', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 217, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed8c88c16462667c3458ecfc451c6e2b', 'text': 'As discussed earlier, 5G brings in a growing number of massive IoT (mIoT) and industrial IoT (IIoT) use cases, which means that the attackers can use them to attack the service provider’s network. DDoS attacks can be inbound and outbound, as explained in the section “The Attacker Takes Control of IoT Devices with Weak Security and Launches DDoS Attack”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 217, 'parent\_id': '7e4a1ded5190c650f697ba0a374ff839', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58897610e863a441d142e74505563701', 'text': 'To secure the network from the inbound attacks from the Internet and the attacks from the consumer IoT devices, which are getting more sophisticated by the day, it is recommended to have a central and distributed protection against DDoS attacks. As illustrated in Figure 4-36, the DDoS protection provided at the edge (such as the MEC layer or the access and aggregation layer) is called distributed Anti-DDoS protection, while the DDoS protection delivered at the centralized DC is called the centralized Anti-DDoS protection.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 217, 'parent\_id': '7e4a1ded5190c650f697ba0a374ff839', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '285a3da3b8e4e8096d0365791abc762a', 'text': '|====p- 3 ---» 4 EEEE (<A>) 3 ;’ [ \_d gNB % : i = & MEC Centralized 4G &5G Packet Core eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 218, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4bf8fee1749caa961cc6803b97efbbb0', 'text': 'Figure 4-36 Centralized and Distributed Anti-DDoS Protection Solution', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 218, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '16508de9cecb9305dfe2b11e10f4254c', 'text': 'Figure 4-37 illustrates the distributed Anti-DDoS mechanism to mitigate the DDoS attack. It allows only legitimate traffic toward the network, thereby securing the 5G infrastructure from inbound attacks from the Internet.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 218, 'parent\_id': '4bf8fee1749caa961cc6803b97efbbb0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f8e98703bb56b208f459b893e473472d', 'text': '> Legitimate Traffic — —» DDoS Traffic S=se= L d " 4—\_—»::- MEC Centralized 4G & 5G ED\_ Packet Core - E-——— e e ((A>) eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 218, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Header', 'element\_id': '9bfb17a014d77aa05bf819d6db53526f', 'text': 'Figure 4-37 Inbound DDoS Attack Mitigation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 219, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0adfc60e11085ce42570927146f7725b', 'text': 'As seen from Figure 4-37, the DDoS protection solution should allow mitigation against volumetric and application-based DDoS attacks in different portions of the service provider’s network and prevent impacting legitimate traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 219, 'parent\_id': '9bfb17a014d77aa05bf819d6db53526f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd57337e8157efaf7eebcd49a384257a0', 'text': 'As seen in Figure 4-38, the distributed DDoS protection solutions using behavioral-based detection and real-time signature creation algorithms that mitigate the DDoS threat vectors at the edge are recommended to be deployed at the edge of the network, such as in the aggregation and pre-aggregation layers of transport or the MEC layer. These algorithms should create baselines of normal network, application, and user behavior and use these baselines to notice abnormal traffic and accurately detect attacks. When a new, previously unknown zero-day attack is detected, the solution should create a signature in real time that uses the attack characteristics and detects known and unknown attacks in a short timeframe, with minimal false positives.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 219, 'parent\_id': '9bfb17a014d77aa05bf819d6db53526f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f83d8decf3ddaea807a62ff1116ba2fd', 'text': '— Legitimate Traffic —> DDoS Traffic | 4 & Internet \\ | \\\\ k/J (Central Anti-DDoS \\ | L ( \\\_ Controller / SR T " o A n)i gNB <+ —XZQBDOS protectios / | 4 — - No— | . — = MEC Centralized | DDoS proleclion)’:/ 4G &5G - Packet Core jg- eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 219, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6b2586c32b7c7869f9cce93f5bfb613b', 'text': 'Figure 4-38 DDoS Attack Mitigation Using Distributed Anti-DDoS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 219, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '253830176ffeff3242ab5c304bf133ad', 'text': 'protection', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 219, 'parent\_id': '6b2586c32b7c7869f9cce93f5bfb613b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '287df101691ec57f841e0169ccd81eef', 'text': 'Security Analytics and Monitoring', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 220, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8bab7d8aa062141264892280505ede8c', 'text': '5G deployments will see stronger adoption of APIs, not only for inter-5G core network function communication, but also for monitoring use cases. It can be seen as an actual replacement of Simple Network Management Protocol (SNMP). The traditional methods of monitoring service provider networks using polling methods such as SNMP, Syslog, and CLI use a pull model to request information at regular intervals. The data collected might help to efficiently monitor the network initially; however, as the network grows in complexity and scale, this method of data collection would be insufficient for efficient and effective monitoring. Additionally, the polling methods are resource intensive, and network operators face information gaps in the data they collect.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 220, 'parent\_id': '287df101691ec57f841e0169ccd81eef', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ad642187726fbea3e6879cdad109d3ef', 'text': 'To mitigate the example threat vectors mentioned in this section, the recommended practice is to have the multivendor telemetry collection from the transport and the RAN infrastructure. Generally, the anomaly detection systems would consume the data collected for around 15 days and generate a baseline for the network. Once the baseline is established, the security analytics and monitoring solution can detect the anomalies. For example, as shown Figure 4- 39, by detecting the IP address being allocated toward the RAN infrastructure, any new host requesting a new IP address can be detected because it shows up as an anomaly. The same applies for the transport layer anomalies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 220, 'parent\_id': '287df101691ec57f841e0169ccd81eef', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '9650fe8bf2419f90d1ba6d791d5c5e12', 'text': 'v \\ Security Analytics & Monitoring ) r = Lo Y <4 gNB 4 = IJ- Centralized 4G & 5G - E-——— c@ - ( = ST Packet Core A))‘ eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 220, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e03c9a833fe98e719e1f7a0ce59f3b8', 'text': 'Figure 4-39 Security Analytics and Monitoring', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 220, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b5247c284a105cbf043c30cd1545735', 'text': 'To avoid each and every new IP address as an anomaly, the anomaly detection system has a list of known IP address allocated in the network and also updates itself with any known or newly configured IP address using its integration with the existing Network Planning and Provisioning solutions already implemented in your network. These solutions would typically have all the IP address allocated to network devices after being authenticated by your Network Access Control (NAC) solution, which enforces policies on devices that access your network or are deployed in your network. The anomaly solution then compares any new IP address to the list of planned or known IP addresses and identifies only the unknown or unplanned IP addresses as anomalies. To reduce the collection of network telemetry from all network switches and routers, it is recommended to collect telemetry from switches and routers that are deployed at aggregation points.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 221, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '52075fc96ea50e990a4acef3a1e263a2', 'text': 'Figure 4-40 shows the network telemetry collection from the network devices in the access and aggregation layer, MEC layer, and the back haul devices. The security analytics and monitoring solution should also create alerts based on any anomaly in network behavior.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 221, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '015e9090c30e1f1271e0eefacc1b48e9', 'text': 'Multi-vendor telemetry collection = » Detect anomalies >< Security Analytics & Monitoring in the network A [ e i \_ ( A)) N o A L d MEC Centralized 4G & 5G - E—— e Packet Core \_( A»‘ eNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 221, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e67ca3da0e721b5e9457f3e733f92dc8', 'text': 'Figure 4-40 Security Analytics and Monitoring in RAN and Transport', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 221, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ed4520070cac80d1f7681be2004ac12d', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 221, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd63da45bd8eccbe8cd99c76361185f6a', 'text': 'As a summary for securing the RAN and Transport infrastructure, the highlighted security controls in Figure 4-41 are recommended.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 221, 'parent\_id': 'ed4520070cac80d1f7681be2004ac12d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'e32fd4338430f41c9d8898179fc886ed', 'text': '~Y YT b Internet V S (8 2 I L d NE o = i 3 ; Centralized 4G & 5G Packet Core -0 <(A)‘ eNB Spectrum Analyzer Jamming Detectors Built-in HW and SW security layer , SZTP Rogue/fake RAN node detection Enhanced Access Control layer Security Gateway and DDoS layer Secure Analytics and Monitoring', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 222, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3e65ebb08702cbd630b7460a440e2572', 'text': 'Figure 4-41 Multilayered Security Controls for RAN and Transport', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 222, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3c6a1e61bc5db54334a98cf19a18e19a', 'text': 'As Figure 4-41 illustrates, a range of security controls is required to secure the air interface, RAN, and Transport layer. Just having a single security control is not enough to cater for the RAN and transport security. The security controls highlighted in Figure 4-41 are not unique only to the RAN and Transport layer but can be re-applied to other domains such as DC and 5GC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 222, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fd2f1555f4980bc9a6e5a1942b76ddfb', 'text': 'Here’s a summary of the controls for securing the air interface, RAN, and transport layer:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 222, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6f97ca975964ca0a0c03ac04510f374a', 'text': '• Built-in hardening: The built-in security of the device based on hardware (HW) and software (SW) hardening is quite critical to prevent DDoS attacks happening within the network. This could happen due to updates that could be infiltrated with malicious code, which might then cause vulnerabilities in all the transport devices being updated. This vulnerability could then be exploited by the attackers. This makes inherent hardware and software hardening by vendors very critical and is strongly recommended to be used by the vendors being chosen for the transport access devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 222, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e23a23d202a840e3f6ef8370113381de', 'text': '• Spectrum analyzer and the jamming detectors: These security controls are unique to the air interface layer and would help in the detection of the air interface jamming systems.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 223, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c5359a79a625531abea5be165e7d36cc', 'text': '• Rogue/fake node detection: The detection of the rogue/fake RAN node is made possible by monitoring the KPI and the UE measurements and then detecting the anomalies, as mentioned earlier in the chapter. The detection of fake nodes applies to the transport nodes, and security policies such as communication only between trusted devices should be applied in the network. This is provided by some vendors offering transport access and aggregation routers that check whether or not the next-hop router is trusted. The data packet would be passed to the next hop only if its trusted.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 223, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '956a1b37b0ff0b0b418e2e482293dcae', 'text': '• SZTP: It is recommended that Secure Zero-Touch Provisioning (SZTP) be used for all devices being deployed in the 5G infrastructure. For this section, it includes the RAN components depending on deployment, such as the gNB, DU, and CU, and the transport elements, such as front-haul, mid-haul, and back-haul routers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 223, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '830aa9bff5dc9e7e61519a7e7b181f6d', 'text': '• Granular access control layer: Granular access controls following Zero Trust principles are recommended to be included as part of the initial deployment plan for the RAN and transport layer. Role-based access control (RBAC) should be provided by the vendor, which can be integrated with the multifactor authentication (MFA) solution. The MFA solution should check the health of the device before the user and the device are allowed access into the network. Specifically, for virtualized components, such as any applications deployed on the programmable access and aggregation routers, it is important to have the user-to- application mapping. It should have a default rule of rejecting any request by default and allowing only specific user requests, which includes rules for API calls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 223, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '120ac084487218ae1aa6c9b02f19140e', 'text': '• Secure analytics and monitoring: The secure analytics and monitoring layer should include the anomaly detection algorithms and should be able to ingest global threat intelligence. This solution should be able to consume multivendor flows such as NetFlow, jFlow, sFlow, IPFIX, Syslog, and so on, and baseline the network after observing the network for 2 to 3 weeks. This includes the user accessing specific devices or applications. Once the baseline is finalized, it will used as a threshold for normal behavior of the network. Any variation from this baseline will be', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 223, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a8d1fdd1484d2a7015610706c10d93e8', 'text': 'considered an anomaly and should be brought to the attention of the relevant teams. The monitoring should also be catered for encrypted traffic without having to decrypt it. This is provided by vendors in the market today and is basically done by understanding more details in the header of the packet.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 224, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '19b479362a0f7b883a6a3b4127a8b11e', 'text': 'Acronym Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 224, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '8c678eeae1091f493e1a9da7290f5956', 'text': 'Acronym Expansion 5GC 5G core AH Authentication Header AKA Authentication and Key Agreement AS Access Stratum CNF Cloud-Native Function Ccp Control plane CU Centralized unit CuPS Control Plane User Plane Separation C-RAN Cloud RAN or Centralized RAN or Central RAN DDoS Distributed denial of service DL Down link DoS Denial of service DU Distributed Unit EAP Extensible Authentication Protocol ESP Encapsulation Security Payload FH Front haul GUTI Global Unique Temporary Identifier IKE Internet Key Exchange IMSI International Mobile Subscriber Identity', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Acronym</th><th>Expansion</th></tr></thead><tbody><tr><td>5GC</td><td>5G core</td></tr><tr><td>AH</td><td>Authentication Header</td></tr><tr><td>AKA</td><td>Authentication and Key Agreement</td></tr><tr><td>AS</td><td>Access Stratum</td></tr><tr><td>CNF</td><td>Cloud-Native Function</td></tr><tr><td>Ccp</td><td>Control plane</td></tr><tr><td>CU</td><td>Centralized unit</td></tr><tr><td>CuPS</td><td>Control Plane User Plane Separation</td></tr><tr><td>C-RAN</td><td>Cloud RAN or Centralized RAN or Central RAN</td></tr><tr><td>DDoS</td><td>Distributed denial of service</td></tr><tr><td>DL</td><td>Down link</td></tr><tr><td>DoS</td><td>Denial of service</td></tr><tr><td>DU</td><td>Distributed Unit</td></tr><tr><td>EAP</td><td>Extensible Authentication Protocol</td></tr><tr><td>ESP</td><td>Encapsulation Security Payload</td></tr><tr><td>FH</td><td>Front haul</td></tr><tr><td>GUTI</td><td>Global Unique Temporary Identifier</td></tr><tr><td>IKE</td><td>Internet Key Exchange</td></tr><tr><td>IMSI</td><td>International Mobile Subscriber Identity</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 225, 'parent\_id': '19b479362a0f7b883a6a3b4127a8b11e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '2290287a3bc758351322a36a5d79e413', 'text': 'IPsec IP Security ISAKMP Internet Security Association and Key Management Protocol MAC Medium Access Control MEC Multi-access edge compute MitM Man in the middle mMTC Massive machine type communication NAS Non[nd]Access Stratum NAT Network Address Translation NGAP Next-Generation Application Protocol NR New Radio NSA Non-standalone 0AM Operations Administration Management 0-RAN Open RAN 0O-RU O-RAN Compliant Radio Unit 0-DU O-RAN Compliant Distributed Unit 0-CU O-RAN Compliant Centralized Unit PFCP Packet Forwarding Control Protocol RAN Radio access network RAT Radio access technology', 'metadata': {'text\_as\_html': '<table><thead><tr><th>IPsec</th><th>[P Security</th></tr></thead><tbody><tr><td>ISAKMP</td><td>Internet Security Association and Key Management Protocol</td></tr><tr><td>MAC</td><td>Medium Access Control</td></tr><tr><td>MEC</td><td>Multi-access edge compute</td></tr><tr><td>MitM</td><td>Man in the middle</td></tr><tr><td>mMTC</td><td>Massive machine type communication</td></tr><tr><td>NAS</td><td>Non[nd]Access Stratum</td></tr><tr><td>NAT</td><td>Network Address Translation</td></tr><tr><td>NGAP</td><td>Next-Generation Application Protocol</td></tr><tr><td>NR</td><td>New Radio</td></tr><tr><td>NSA</td><td>Non-standalone</td></tr><tr><td>0AM</td><td>Operations Administration Management</td></tr><tr><td>0-RAN</td><td>Open RAN</td></tr><tr><td>0O-RU</td><td>O-RAN Compliant Radio Unit</td></tr><tr><td>0-DU</td><td>O-RAN Compliant Distributed Unit</td></tr><tr><td>0-CU</td><td>O-RAN Compliant Centralized Unit</td></tr><tr><td>PFCP</td><td>Packet Forwarding Control Protocol</td></tr><tr><td>RAN</td><td>Radio access network</td></tr><tr><td>RAT</td><td>Radio access technology</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 226, 'parent\_id': '19b479362a0f7b883a6a3b4127a8b11e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '889e0debf9a6ac97ff3c9e008b58f7ee', 'text': 'RLC Radio Link Control RRC Radio Resource Control SA Standalone SCTP Stream Control Transmission Protocol SDN Software-defined network SecGW Security gateway SEG Security gateway SUCI Subscription Concealed Identifier SUPI Subscription Permanent Identifier SZTP Secure Zero-Touch Provisioning UE User equipment UL Up link upP User plane URLLC Ultra-reliable low-latency communication VRAN Virtual RAN TP Zero-Touch Provisioning', 'metadata': {'text\_as\_html': '<table><thead><tr><th>RLC</th><th>Radio Link Control</th></tr></thead><tbody><tr><td>RRC</td><td>Radio Resource Control</td></tr><tr><td>SA</td><td>Standalone</td></tr><tr><td>SCTP</td><td>Stream Control Transmission Protocol</td></tr><tr><td>SDN</td><td>Software-defined network</td></tr><tr><td>SecGW</td><td>Security gateway</td></tr><tr><td>SEG</td><td>Security gateway</td></tr><tr><td>SUCI</td><td>Subscription Concealed Identifier</td></tr><tr><td>SUPI</td><td>Subscription Permanent Identifier</td></tr><tr><td>SZTP</td><td>Secure Zero-Touch Provisioning</td></tr><tr><td>UE</td><td>User equipment</td></tr><tr><td>UL</td><td>Up link</td></tr><tr><td>UP</td><td>User plane</td></tr><tr><td>URLLC</td><td>Ultra-reliable low-latency communication</td></tr><tr><td>VRAN</td><td>Virtual RAN</td></tr><tr><td>TP</td><td>Zero-Touch Provisioning</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 227, 'parent\_id': '19b479362a0f7b883a6a3b4127a8b11e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '186d95e08c7810ba5051cdc2e24d6f80', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 227, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '09129ad2d21a9b23f499cc31f82ddffd', 'text': 'IETF RFC-4303, “IP Encapsulating Security Payload (ESP)” IETF RFC 8221, “Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 227, 'parent\_id': '186d95e08c7810ba5051cdc2e24d6f80', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '02cc1682f52962fe222dee9d4b7a628a', 'text': '3GPP TS 33.501, “Security architecture and procedures for 5G system,” Release 16, v 16.5.0, December 2020.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 227, 'parent\_id': '186d95e08c7810ba5051cdc2e24d6f80', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd84e6524b7687c9968f0024bb94a5753', 'text': '3GPP TS 33.201 V16.4.0, “Network Domain Security (NDS); IP network layer security,” Release 16', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 227, 'parent\_id': '186d95e08c7810ba5051cdc2e24d6f80', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1c9b0cea98cd3f592839362f2f25a97a', 'text': '3GPP TS 33.809 V0.11.0, “Study on 5G Security Enhancement against False Base Stations (FBS),” Release 17', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 228, 'parent\_id': '186d95e08c7810ba5051cdc2e24d6f80', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ca805f43b98059d17e6fbdedbf23ede1', 'text': 'O-RAN Alliance white paper, “O-RAN Minimum Viable Plan and Acceleration towards Commercialization,” June 2021', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 228, 'parent\_id': '186d95e08c7810ba5051cdc2e24d6f80', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '133dfb42f07ac9a46cedc2b3f116fda8', 'text': 'Pramod Nair, “Securing 5G and Evolving Architectures,” Cisco Knowledge Networks, Cisco Public, September 17, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 228, 'parent\_id': '186d95e08c7810ba5051cdc2e24d6f80', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e33e332565c3242a7a3d03440d5e7c7b', 'text': 'Pramod Nair, “Why 5G is changing our approach to security,” Cisco Public, June 10, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 228, 'parent\_id': '186d95e08c7810ba5051cdc2e24d6f80', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '16eb83b1c7117751074ebf01da62308b', 'text': 'https://www.cisco.com/c/dam/en/us/solutions/collateral/service- provider/mobile-internet/solution-overview-c22-741906.pdf', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 228, 'parent\_id': '186d95e08c7810ba5051cdc2e24d6f80', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '31c8ad428df9e1dcf353d1657835e1c1', 'text': 'O-RAN Security Threat Modeling and Remediation Analysis 1.0, March 2021', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 228, 'parent\_id': '186d95e08c7810ba5051cdc2e24d6f80', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9fb78f42154bdcac94dd3027a360b935', 'text': 'Chapter 5. Securing MEC Deployments in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd834897e0ff155bd3024da376647ef20', 'text': 'After reading this chapter, you should have a better understanding of the following topics:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8837a4b3ab17b342c7ff1f347136a946', 'text': '• Key threat surfaces in different models of 5G MEC deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9d7f5e16c44e77faedafd29375100331', 'text': '• Key security controls for securing 5G MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '13dd272a7f224e9146f90f006153fa5d', 'text': '• Real scenario case study examples on MEC threat surfaces and threat mitigation techniques', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd82f0bbbe494ac8d072f46ade3c83d3a', 'text': 'In the previous chapters, we discussed the security controls to mitigate threat surfaces in 5G radio access network (RAN) deployments. This chapter will take you through the threat surfaces in 5G multi-access edge computing (MEC) deployments and mechanisms to mitigate the threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e8336da2d24382e6973c25fe0efc526a', 'text': 'This chapter will be of particular interest to the following teams from enterprise 5G MEC consumers, 5G service providers, and cybersecurity vendors providing security layers for MEC deployments:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36c128348d2749651e4ed084b2ff10f2', 'text': '• Mobile infrastructure strategy teams of service provider and enterprise verticals deploying 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b7cd520f99a77cb3b37ed58ffce303ec', 'text': '• Security strategy teams within service provider and enterprise verticals deploying 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '56972905ac86e6ae271509804b479d79', 'text': '• Radio planning and optimization teams within service providers and private 5G enterprises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e33d1e15dfd932f0b38d1c53c01a0764', 'text': '• Transmission and the packet core team within service providers and private 5G enterprises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '03c2cd3a41b78cdb2761377350bd1992', 'text': '• Cloud computing and data center teams involved with 5G strategy and deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9a07fdbc33597821b0cb025403825544', 'text': '• Security architects and design teams looking at securing the mobile infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9fccabc26266263b8d37571d49ed0f90', 'text': '• Enterprise solution and security architects deploying 5G MEC on enterprise premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 229, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '08e9e85c3b82502663e299fd31a24f26', 'text': '• Enterprise solution and security architects using 5G MEC from a service provider', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 230, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0a67cfe6f78689eba0d3bfbc54523636', 'text': '• Defense personnel deploying 5G MEC for defense use cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 230, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ac56975648ab7f739385d707c5864a4f', 'text': '• Government departments deploying 5G MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 230, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '338a38f677334d3de02ce9026e69017e', 'text': '• Cybersecurity vendor teams looking to secure MEC deployments for their customers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 230, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6bf7c7cab795e5eeef3260c419b0eb2c', 'text': '• Product managers of cybersecurity vendors', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 230, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3c53b50e1d8cb393667c7cfe044b159a', 'text': '• Consultants working on MEC strategy', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 230, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '04098bcefefb60b68c4d4e1962a6662c', 'text': 'Multi-access edge computing (MEC) is an architecture concept defined by the European Telecommunications Standards Institute (ETSI) that enables deployment of cloud computing and IT services at the edge of the network. The fundamental idea here is that moving the application and the processing of the traffic closer to the user reduces the latency for the end user of the application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 230, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3546276dbac39ab3fa7a2ce3e7c6ec28', 'text': 'MEC is technology-agnostic and opens up the ecosystem to many different areas, such as cloud computing, software-defined networking (SDN), application developers working on artificial intelligence (AI), Internet of Things (IoT), and the delivery of content with local cache and real-time analysis of data, by opening up the applications deployed on the network edge to the third-party application ecosystem in the public cloud. This is done as MEC architecture specified by ETSI uses open interfaces such as Representational State Transfer (REST) application programming interfaces (APIs) for the exchange of data.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 230, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5f6663587708a4877dbbed8d8475f99c', 'text': 'MEC discussions are becoming more prevalent within service providers due to 5G use cases such as massive IoT (mIoT) and machine-to-machine (M2M). MEC enables disaggregation and distribution of 5G RAN and 5GC (5G packet core). You can now deploy the 5G RAN functions such as Distributed Unit (DU) and Centralized Unit (CU) and the user plane 5GC functions such as User Plane Function (UPF) in the edge of the network to provide faster and high-bandwidth applications to its subscribers. These 5G functions require to be deployed dynamically for optimal use of resources, which is enabled with features such as virtualization, SDN, and orchestration.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 230, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '16ec0df700d0e0cc8cc69ee862567321', 'text': 'MEC is also becoming more prevalent in enterprise networks, as the enterprise infrastructures are growing in complexity, accommodating more and more diverse, end-user devices and IoT connections. Today’s applications are more interactive and bandwidth hungry, generating massive amounts of data that', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 230, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f3a2d021e0685928aa8321d4915d3f3a', 'text': 'supports real-time analytics and problem solving. Many enterprises have adopted multicloud strategies with unified management solutions to support microservices and containerized applications at the network edge with more distributed and intelligent edge network capabilities with constantly evolving security. Edge networks and computing allow enterprise architectures to optimize processing for business-critical analysis of data sets from IoT applications and communications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 231, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f6fb5d0cb28a321a38a381c202e1037c', 'text': 'The MEC ecosystem also includes container-based platforms implemented on OpenStack and other cloud-native container platforms, enabling open source edge computing and IoT cloud platform optimized for low-latency and high- performance applications. There are lot of innovations happening in MEC related technologies such as MEC service-chaining. As an example of MEC service chaining, instead of having separate hardware equipment specific for security controls such as Firewalls, DDoS protection, load balancers and so on, all these security controls and network functions such as UPF can be deployed as virtual components on a scalable commercial off the shelf (COTS) server with integrated orchestration and automation components. This brings in advantages related to lower energy consumption when compared to traditional network deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 231, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3c5e3a861d836a1735d3162b0b563eea', 'text': 'Here are the key advantages of following the MEC architecture deployment:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 231, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6a3855844112029e19ff61c39a9f8cf7', 'text': '• Enabling optimized DC deployment using distributed cloud computing and IT service in edge functionalities of MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 231, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2fd7830214093b7e2e828c4c5cdcf94f', 'text': '• Enabling ultra-reliable low-latency communication (URLLC) use case deployment, which targets latency of 1ms', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 231, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fcceef8d744704aeb0ef2c734fe8d59a', 'text': '• Reducing the traffic in the back haul by optimized traffic offload in the MEC design, allowing Direct Internet Access (DIA) and Local Break Out (LBO)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 231, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '579343572ed679496f6897f3acc59a71', 'text': '• Better quality of experience (QoE) for end customers by utilizing the edge cache functionality using MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 231, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e522661d49d6b5121990229df01b2b92', 'text': 'Two primary MEC architectures are being planned by service providers and enterprises:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 231, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd0bcbbe6f725a886fa045a4518f23862', 'text': '• Service provider network-based MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 231, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7d80d224d79ba880fc5a0a522c589ec1', 'text': '• Enterprise network-based MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 231, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4e1186759a309ae26d1d762e57cdeed5', 'text': 'The sections that follow describe these in more detail.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 231, 'parent\_id': '9fb78f42154bdcac94dd3027a360b935', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ca3b2fd2787ca57422360731f7eeb6b8', 'text': 'Service Provider Network-Based MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ef51db9034449a954f614343e5386ad2', 'text': 'This model is used by service providers to enable 4G and 5G networks. Here, user plane functions and certain MEC applications are deployed in the edge to allow better QoE for subscribers as well as optimized traffic volume in the back haul by using the DIA and LBO functionalities of the MEC. In telco environments, OpenStack is seen as the main platform to host the container running in the environment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'parent\_id': 'ca3b2fd2787ca57422360731f7eeb6b8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd5f5d31f2dbc1de939b3176b54be2bbf', 'text': 'Figure 5-1 shows the key components of service provider network-based MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'parent\_id': 'ca3b2fd2787ca57422360731f7eeb6b8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '54dbeeab297414b58ccd088425a0fb4e', 'text': 'Virtualized infra (ex: containers, VM, NFVi ST S S e SR MANO, UPF, MEC Applications) O &om loT Applications, processing and storage ( A)) Eeoeas e e e : APIs to Cloud deployed application and MEC I SP services , Direct Internet Access (DIA) S §', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f1c68ca2f15d7d5d205ab9f4ff5837ba', 'text': 'Figure 5-1 Service Provider Network-Based MEC in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6e4a71822b553a19c73c9c7f25d00464', 'text': 'Examples of use cases include the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2983a741a3e5271e3fa8162a5d64fe93', 'text': '• Enabling distributed CUPS deployment of 4G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8193ffc80c9e50ecffd374922e5f7303', 'text': '• Enabling distributed, disaggregated RAN components—DU and CU', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f9381978a962c1f2c68ea9ec2f609964', 'text': '• Enabling distributed deployment of 5GC by enabling virtualized UPF deployment closer to the edge', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1345be54e34914f53740347e8ea2fc51', 'text': '• Efficient deployment of IoT by enabling data processing and “noisy signaling” IoT use cases at the edge instead of the cloud', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '388c231cb1d301b77bfa9d694111ae85', 'text': '• Deployment of URLLC use cases at the edge', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e1c8d642f67b62f25f1e19e27d8147de', 'text': '• Deployment of vehicle-to-everything (V2X) applications in the edge', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '758caf0be7e2f949ecdb21c2c95e2af6', 'text': '• Deployment of applications and services at the edge for monetization', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fd5c4ffa29578a47a2a474b66676c184', 'text': '• Enabling high-bandwidth use cases such as video streaming in eMBB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 232, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5768d645244e46c10473af14e9bb4ada', 'text': 'Enterprise Network-Based MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fb3106407b88e7d22a69f4ad317e6f8f', 'text': 'The enterprise network-based MEC model is used by enterprises to fulfill use cases such as deploying private 5G (non-public 5G networks) to reuse the service provider’s infrastructure. It can also be used by service providers to offer certain services from the edge to the enterprises.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'parent\_id': '5768d645244e46c10473af14e9bb4ada', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '00551fc9c47826c18b1c67062048bf43', 'text': 'Figure 5-2 shows the key components of enterprise network-based MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'parent\_id': '5768d645244e46c10473af14e9bb4ada', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '7b5fb009abfb61385f76b4cf52c3a466', 'text': 'Virtualized infra (ex: containers, VM, NFVi PR e e S l MANO, UPF, CU, DC - ©&ciE Enterprise applications (ex: M2M config, performance and fault management) ( A)) e B e e e i APIs to enterprise private cloud deployed application, Direct Internet Access (DIA) MEC § I f', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0009c4b73b4c4d54247191ff07b7bcef', 'text': 'Figure 5-2 Enterprise Network-Based MEC in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '17653db19e1c6dc3bcede77008bbf7c9', 'text': 'Example of use cases include the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '83f93e2e07fd062a90458e1e701fbed7', 'text': '• Edge deployment of IoT devices with high-traffic volume in enterprise networks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6a63bb30aa5f47a79c86a38d2aa1c39d', 'text': '• M2M/robotics use cases in manufacturing sector.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f724927680e8728e836afee492df0aed', 'text': '• Industrial IoT use cases such as real-time information.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d3a6192e48a3612a3f4d2bfbe05f9e9', 'text': '• Streaming content use cases in the enterprise, including augmented reality (AR) and virtual reality (VR).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f3687a382cdaa294a8f6dfc141ea4cbe', 'text': '• Location-limited use cases such as assets restricted to certain locations.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a13be0948acca95618aa360f3dd835c3', 'text': '• Healthcare use cases where data privacy is important and deployed on the edge network of the healthcare vertical. Only non-private data is sent between the edge and the central DC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2efeef2143fa7fc42d8a88f8303da0c2', 'text': '• Smart city use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1b9fbf2dd3c57715fd6c0cfae6fe3489', 'text': '• AI and edge computing use cases focusing on leveraging AI to enhance automated processes and analytics data interpretation necessary to support', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 233, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3179cf6d560eef1ecd9f8c4f15b47f0d', 'text': 'ultra-low latency application delivery and to alleviate network congestion in core data centers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 234, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c3d8889c4b555f55f61ae748c4a56987', 'text': 'MEC Deployment Models', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 234, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '98e8cd1f9ad92e66ca936b5e12209ecd', 'text': 'MEC is not a new concept for 5G. It was used in distributed mode deployment of 4G Control Plane User Plane Separation (CUPS). 4G CUPS gave us the option of separating the user plane (UP) and control plane (CP). If the UP and CP are deployed in the same location, it is called a co-located CUPS architecture. It could also be deployed in distributed mode; if the user plane is deployed closer to the edge of the architecture and the control plane is deployed at the centralized data center (DC), it is then called a distributed CUPS deployment. The control plane, which is less sensitive to latency, was deployed in the centralized data center, and the latency-sensitive user plane was deployed in the edge. Some use cases of IoT, which are not latency sensitive, can have the user plane deployed at the central DC as well.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 234, 'parent\_id': 'c3d8889c4b555f55f61ae748c4a56987', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '87fdbf9a9cda727b46c80bbcc7c65518', 'text': 'Figure 5-3 shows the key control plane and user plane components of 4G architecture from a RAN integration point of view.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 234, 'parent\_id': 'c3d8889c4b555f55f61ae748c4a56987', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f6d476dd5c1b167a47581958335f7d3d', 'text': "St <<A> ! eNB ¢ S1-U dBb o saw }‘E'[ PGW ¢ SGi SP Applications & Internet", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 234, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4605670afdc70afaa841111a7b97d481', 'text': 'Figure 5-3 Key Control Plane and User Plane Connections for 4G RAN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 234, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd772fc4f59666d3d646ad1ee6e2bfe5b', 'text': 'Figure 5-3 depicts the control plane and user plane in 4G architecture. The S1 interface in LTE is used between LTE RAN nodes eNodeB (eNBs) and the Evolved Packet Core (EPC) nodes MME and S-GW. The S1 interface includes the S1-CP (control plane) and S1-UP part (user plane). The signaling transport on S1-CP will be based on SCTP. The signaling protocol for S1 is called S1- AP. The user plane interface is based on GTP User Data Tunneling (GTP-U).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 234, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c6a53424f869d5c06f5eba9afa7f091e', 'text': 'Figure 5-4 shows the key Control Plane and User Plane Separation (CUPS) of the 4G architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 234, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '8618e655c6419cf11a4572a37b9fee10', 'text': 'Control Plane User Plane separation / Control Plane S$1-C—— MME }gﬁﬂsey- CJ?;ET[PGY-CW/ S>‘(a Sxb ’ . User Plane 3\\ ( A)) i A4 S1-U eNB () {PaW- U sai dBb SP Applications & e M R LT Sy S Internet', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 235, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '588571af83359491ce12d3cefb414ea4', 'text': 'Figure 5-4 Control Plane and User Plane Separation in 4G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 235, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d032b49f3056a9eb4ad248cfc310c9c', 'text': 'The mobile network today started seeing increased variation in resource demands across the control and user planes. Some devices are high control plane resources (signaling), while other devices might require very little signaling resources but substantial user plane and data resources. As Figure 5-4 illustrates, the introduction of CUPS addressed this to a certain degree. CUPS offers the capability to truly separate and independently scale the control plane and user plane of the mobile network on an as-needed basis and in real time. You now have the flexibility to specialize the user plane for different applications, without incurring an associated cost of a dedicated control plane for each application. New use cases such as remotely operated machinery, edge computing, and ultra-high per-user throughput will now be possible due to this distribution of control plane and user plane as well as the flexibility to deploy closer to the edge. Finally, CUPS enables you to optimize data center costs by hosting the control plane and the user plane in different geographic locations as well as save on back-haul costs by terminating data at the edge of the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 235, 'parent\_id': '588571af83359491ce12d3cefb414ea4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '79184c948efa7481df8ab125e32eba6c', 'text': 'In a CUPS deployment, the SGW and PGW are decomposed into separate control plane and user plane components. The SGW is decomposed into SGW- C and SGW-U, and the PGW is decomposed into PGW-C and PGW-U. Figure 5-4 also illustrates the involvement of new network elements for the control plane, such as SGW-C and PGW-C, and the user plane, such as SGW-U and PGW-U. The functions of these new network elements in 4G CUPS are listed here:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 235, 'parent\_id': '588571af83359491ce12d3cefb414ea4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '241a860980d3e3d60fa9618fd9915f4d', 'text': '• SGW Control Plane (SGW-C): SGW-C performs the control plane functionality for the assigned SGW-U in a 4G CUPS deployment. The user equipment (UE) is served by a single SGW-C, but multiple SGW-Us can be selected for different Packet Data Network (PDN) connections. SGW-C also supports triggering downlink data buffering while the subscriber is being paged, PGW pause of charging management based on implemented policies (failed paging, abnormal radio link release, and dropped packets/bytes at SGW-U), and lawful interception of subscriber traffic. It supports the Sx interface, which enables CUPS between SGW-C and SGW-U.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 236, 'parent\_id': '588571af83359491ce12d3cefb414ea4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cc58bb59bf1919082ad99df69487710c', 'text': '• SGW User Plane (SGW-U): SGW-U performs the user plane functionality of the SGW in a CUPS deployment. It consists of an S1 data plane stack to support the S1 user plane with eNodeB. SGW-U also supports triggering downlink data buffering while the subscriber is being paged and lawful interception of subscriber traffic. It supports the Sx interface, which enables CUPS between SGW-C and SGW-U.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 236, 'parent\_id': '588571af83359491ce12d3cefb414ea4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e6770ab2e380e264bdee8d4159e648ef', 'text': '• PGW Control Plane (PGW-C): PGW-C performs the control plane functionality of the PGW in a CUPS deployment. When a subscriber establishes an EPS (Evolved Packet System) bearer to a given PDN, the PGW-C selects and controls the point of attachment to that PDN for the life of the EPS bearer. PGW-C caters for resource management for bearer resources, bearer binding, subscriber IP address management, and mobility support.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 236, 'parent\_id': '588571af83359491ce12d3cefb414ea4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '49ac6765e31dbda0e9ead6fee7fc657c', 'text': '• PGW User Plane (PGW-U): PGW-U serves as user plane functionality of the PGW in a CUPS deployment. When a subscriber establishes an EPS bearer to a given PDN, the PGW-U under the control of the PGW-C serves as the point of attachment to that PDN for the life of the EPS bearer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 236, 'parent\_id': '588571af83359491ce12d3cefb414ea4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8e13bc8e68d5c7ec7d9a358a7bdc7056', 'text': 'For use cases that are low-latency dependent, you can deploy the user plane functions such as SGW-U and PGW-U closer to the edge in a remote data center or MEC node so that the control plane functions can be deployed in the centralized DC. This is because the latency is user plane latency dependent and less sensitive to control plane latency. This CUPS deployment will allow you to implement the use case by keeping the cost in check, as the resources in the remote DC or MEC node are not consumed for control plane functions. Expensive upgrades such as back-haul upgrade can be avoided while using CUPS architecture, as the remote DC or MEC can implement Direct Internet', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 236, 'parent\_id': '588571af83359491ce12d3cefb414ea4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3bfffb27a52b8cdf4da970ac6c8dca35', 'text': 'Access (DIA) or Local Break Out (LBO), where the user plane traffic exits out to the Internet from the edge DC using SGW-U and PGW-U and does not require the traffic to be back-hauled to the centralized DC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 237, 'parent\_id': '588571af83359491ce12d3cefb414ea4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '590d32b67b51bf5b992f0813a8dbe196', 'text': 'Figure 5-5 shows a deployment example of 4G CUPS architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 237, 'parent\_id': '588571af83359491ce12d3cefb414ea4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '47c39916037546b8e2af527632838fa1', 'text': '4 SR e S RO o SP Applications & PGW-U Inte;net SGi () SGW-U S1-C <+—51,X2 Sx gNB e = ﬁ@ OAM MEC e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 237, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '357e22dcad736b946768dc4db0042fdf', 'text': 'Figure 5-5 CUPS Deployment in 4G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 237, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c99ab584e28364ca772ec8fd3efa732b', 'text': 'Figure 5-5 shows the distributed deployment of user plane and MEC applications. It provides you with the capability to truly separate and independently scale the control plane and user plane of the mobile network on an as-needed basis and in real time, providing the flexibility to specialize the user plane for different applications, without incurring an associated cost of a dedicated control plane for each application. New use cases, such as remotely operated machinery and ultra-high per-user throughput, are now possible by deploying the user plane on the MEC. Finally, CUPS enables you to optimize data center costs by hosting the control plane and the user plane in different geographic locations as well as save on back-haul costs by terminating data at the edge of the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 237, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9dc33507861833f934f98703a6b8a251', 'text': 'The introduction of 5G brought huge improvements in bandwidth and latency and the capability to tailor service experiences across different vertical markets and individual users. Applications that harness these capabilities can transform industries such as manufacturing, automotive, healthcare, and transportation. To deliver the high-quality experiences that consumers of 5G services expect and demand, there is a need to fundamentally reimagine the service edge. 5G also introduces disaggregation and distribution of RAN components. 5G RAN can be decomposed into CU and DU, which can be deployed as virtual', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 237, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9585f2fde3c2c4a95f8d78fc7d3bda2b', 'text': 'elements in the service edge nodes/MEC. As illustrated in Figure 5-6, the control plane functions are Access and Mobility Management Function (AMF) and Session Management Function (SMF), and the user plane function of 5GC is the User Plane Function (UPF).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 238, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '64cd664e2361f76e5fe2cee3accbbafd', 'text': "o SMF N2 \_(>N11 Control Plane (CP) I s e D RN S - AR N4 e ] N3 UPF N6 ( A)>' gNB - User Plane (UP) Sebrie i e LR SP Applications & Internet (re](ou](eu] iR s e e e A e T", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 238, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '083b2b2667ab0ba44ff2d48b8a45aa7a', 'text': 'Figure 5-6 Key Control Plane and User Plane Connections from Next- Generation Node B (gNB)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 238, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c9575bdd4489a855b26ad6020a77d8a8', 'text': 'Figure 5-6 shows the key control plane and user plane components between 5G RAN and 5GC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 238, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9e93e57237177e3a701c523c299d7fc3', 'text': 'The list that follows describes the interfaces in Figure 5-6:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 238, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '81bfc753f1ab633a0422cca46fb5a0b0', 'text': '• Control plane:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 238, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7206475be493b388aa2ca188f2560ebb', 'text': '• N2: This interface uses SCTP (NGAP) and supports control plane signaling between 5G RAN and 5G Core, covering UE context management and PDU session/resource management procedures. N2 being signaling doesn’t impact the low-latency use cases much (depending on the low-latency requirement of the use case) and is therefore normally planned to be deployed in the central DC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 238, 'parent\_id': '81bfc753f1ab633a0422cca46fb5a0b0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e203665196c68f35d47b086d4a94d16e', 'text': '• N4: The interface between the UPF and the SMF. N4 uses the Packet Forwarding Control Plane (PFCP) protocol, which is also used in Sx interface in the 4G CUPS architecture. The location of deployment of the UPF (that is, whether the UPF is co-located with the SMF or is distributed) determines the need for securing the N4 interface using IPsec ESP and IKEv2 certificate-based authentication provided by the SecGW.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 238, 'parent\_id': '81bfc753f1ab633a0422cca46fb5a0b0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4570cf18fe7e74b2909d0a36b4a93f11', 'text': '• N11: The interface between the Access and Mobility Management Function (AMF) and the Session Management Function (SMF). N11 uses the service-based interfaces (SBIs) for the interactions employing RESTful API over HTTP/2.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 239, 'parent\_id': '81bfc753f1ab633a0422cca46fb5a0b0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0c36940fe160348dc0562b516a090d66', 'text': '• User plane:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 239, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a16ebcba54f101ffa9f15b3da0e10fa7', 'text': '• N3: The interface between 5G RAN and the UPF. N3 carries the user plane data from the UE to the UPF. N3 uses the GPRS Tunneling Protocol (GTP) with header extensions for 5G, Segment Routing (SR), and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 239, 'parent\_id': '0c36940fe160348dc0562b516a090d66', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c15da284b98b41efdf44f38404f823dc', 'text': '• N6: The interface between the UPF and the data network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 239, 'parent\_id': '0c36940fe160348dc0562b516a090d66', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fbd65eeaef23a28e624d9c72b739748f', 'text': 'The actual deployment location (far edge/edge/regional/central, and so on) of the control plane and user plane is dependent on the use cases. The key deployment models being considered by service providers are explained in more detail in the section that follow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 239, 'parent\_id': '0c36940fe160348dc0562b516a090d66', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6554c951a6acb777b7b16987353ec087', 'text': 'Distributed UPF and MEC Application Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 239, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '74d4c2682ed72d02655d1369f7499894', 'text': 'Figure 5-7 shows an example of 5G deployment with separated control plane and user plane.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 239, 'parent\_id': '6554c951a6acb777b7b16987353ec087', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f6b5aa5fa07c0d28363d8cd779375ecf', 'text': 'N6 SP Applications & Internet pEA e S Ge TR ) ((A +«—N2,N3 ., E= < N4 o= [ Biing ) g\\B - N9 MEC - e e e s N Centralized 5GC DC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 239, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '206c9e794873f5373b51067c1533b479', 'text': 'Figure 5-7 Example of Deployment Locations for User Plane and Control Plane Functions in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 239, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bd47a4fdd3d2f2e6042ab419687e550f', 'text': 'Figure 5-7 shows the deployment of the UPF (User Plane Function) in the MEC. The 5G control plane functions, such as AMF and SMF, are deployed in', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 239, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '450fdbdec3a594446b14222792187787', 'text': 'the centralized 5GC DC. For services/use cases that are not low latency sensitive, the UPF can be deployed in the centralized DC. This is an example of how service providers are deploying 5G networks with the distribution of the UPF catering for the low-latency use cases closer to the edge, while the control plane functions, which are less susceptible to latencies, are deployed in the centralized DC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 240, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'bac2d4057ed4ccfaa757a6a511d297a7', 'text': 'C-RAN/O-RAN/Open VRAN Deployment Enabled by MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 240, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6da194e56780e79ec150810f572240d6', 'text': 'Figure 5-8 shows an example of distributed 5G RAN and 5GC deployment using components of Open RAN (O-RAN), Open VRAN (Virtual RAN), and Cloud RAN (C-RAN).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 240, 'parent\_id': 'bac2d4057ed4ccfaa757a6a511d297a7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '9a53c0f3d323b574e6e369fbd5b0e04e', 'text': '@l rApps . [t ieric (public cloud) A1 ? ,,,,, v ‘ @ xApps Near Real SP Applications it Time - RIC and Internet . N6 (« w (CAwF ] (CupF ] | s N2 CSF ] (oam) F1 “——N4— FH—» ) E2 = o= [ Biling ] N9 Fér edge MEC MEC Gentralized 56C DC (on-premises)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 240, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b52d572abcd400d492e24895eb471fe4', 'text': 'Figure 5-8 Example of C-RAN/O-RAN/VRAN Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 240, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd85c47240588d18c62932e0dd82d54e9', 'text': 'Note that the DU can be co-located with the CU but is shown separate in this figure, as it could be one of the deployment options. This architecture using MEC is becoming more popular as service providers explore options of flexible deployment of RAN and reduce cost of densification in terms of transport deployments. The new cloud RAN architecture addresses, among other things, the challenges of building multivendor networks and harmonizing to a common feature set. Applications represent an extension of a RAN Intelligent Controller, which can be deployed in the on-premises or public cloud MEC based on the use case. The applications can be either an xApp for the Near-Real Time RAN Intelligent Controller (Near-RT RIC) or an rApp for the Non-Real-Time RAN Intelligent Controller (Non-RT RIC). xApps are the applications for near real time, such as radio resource management (RRM) and radio optimization algorithms to improve the near-real-time functionalities, which have a latency dependency between 10ms and 1 second. rApps are the applications for non–real time that can support a latency requirement of more than 1 second, such as enriching the information collected by xApps to provide enhanced optimization to the RAN. Applications in these two different environments have different platform mechanisms; however, they share a common behavior of allowing an abstraction layer to provide the capability for the application to be developed such that it can be deployed to either environment from the same package.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 241, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0857fafd36aa3ef0f44dbecdc4df20da', 'text': 'Enterprise MEC Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 241, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '71789e2d7702b3c4d470eff9d0a044a5', 'text': 'Figure 5-9 shows an example of MEC deployment in the enterprise.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 241, 'parent\_id': '0857fafd36aa3ef0f44dbecdc4df20da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '895c4a688d4f23d5603a162b0bd0d670', 'text': 'SP Applications and Internet = ( A)) \_< MEC Centralized gNB 5GC P Enterprise Network | R ) Private | ; (non-Public) = gNB 1 Enterprise MEC DC N | Internet', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 242, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'dbd45bc85fdf53d93aad05850753c09b', 'text': 'Figure 5-9 Example of Enterprise MEC Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 242, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f2bb04dd9b0a30b84cdf1e30155dd679', 'text': 'Apart from the service provider–based MEC, the key use cases of MEC are to enable key 5G use cases such as M2M. Depending on the M2M use case, the enterprise might require a non-public deployment of 5G RAN nodes, user plane functions, and the MEC application such as application interacting with the M2M use case to be deployed within the enterprise perimeter, most probably within the existing enterprise data center. The control plane functions could be deployed in the centralized DC of the service provider or within the same enterprise DC where the UPF are deployed. A majority of service providers are leaning toward the model of having the CP functions of the 5G deployed in the centralized DC and the UP functions within the enterprise DCs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 242, 'parent\_id': 'dbd45bc85fdf53d93aad05850753c09b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '00dd9090de7161d5194e200d54e9d2d4', 'text': 'A majority of enterprises also seem to be leaning toward this model as they have to cater only for their primary services, which require the UP and MEC applications to be deployed in the enterprise DC. The operations, administration, and management (OAM) of the M2M devices is provided by the M2M vendor, and hence the need for the integration arises only for the CP', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 242, 'parent\_id': 'dbd45bc85fdf53d93aad05850753c09b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3bba5d37bd00ea87e130f2951d0ce304', 'text': 'function messages between the enterprise DC and the service provider DC. Few enterprises are also planning to have the entire 5GC ecosystem, including the gNB, UP, and CP, all deployed within the enterprise DC or using a public cloud provider to host all the 5G UP and CP network functions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 243, 'parent\_id': 'dbd45bc85fdf53d93aad05850753c09b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b45d844264834811b4d30dc259ffdaf1', 'text': 'While technically all the mentioned options are viable, the key criteria are cost along with scalability and flexibility. Having the entire 5G network functions owned by the enterprise brings in additional cost for deployment and day-to- day operations, while having a split model allows enterprises to realize the use cases by deploying only the necessary 5G network functions while offloading the non-necessary network functions to be catered by the service provider.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 243, 'parent\_id': 'dbd45bc85fdf53d93aad05850753c09b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '194d98061f825679de51c5d7314d392e', 'text': 'Hybrid MEC Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 243, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '59f49126590390e8c307188a37e4c754', 'text': 'Figure 5-10 shows an example of hybrid MEC deployment that utilizes both public cloud and private cloud infrastructures to make the best use of both infrastructures.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 243, 'parent\_id': '194d98061f825679de51c5d7314d392e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '7f03c794f2001abfd767d9398ce4eb3f', 'text': "Y () CU, UPF 5GC CP (AMF, SMF, PCF ....) 5G edge services & 5G core services & Internet Internet cessassas P ' NMS (EMS B Service provider o= gjling, (<A>) Service Provider P B SR e backhaul e S = Orchestration gNB Front Haul / Mid Haul Centralized 5GC MEC-Compute & storage", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 243, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cb1ea1c209c2e8b98f24f2c52b71db60', 'text': 'Figure 5-10 Example of Hybrid MEC Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 243, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eebf00f1bf1e2ccb96b1024f5009ff35', 'text': '5G also provides the option of closer interaction between public cloud providers and the service providers due to the cloud-native function (CNF) capability of 5G network functions. All the 5G network functions should be capable of cloud native, which means it could be deployed in any infrastructure, including cloud. A majority, if not all of the 5G CNFs are based on open source components. This allows any cloud provider to create their own version of 5GC network functions or partner with any of the 5GC vendors.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 244, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '81d4e47b9afeefd8be68297d8d5744db', 'text': 'Depending on the public cloud provider, there are different options of deploying the 5G network functions using public cloud. One of the options of deploying the 5GC in the public cloud is to deploy the UP and CP 5GC network functions in the public cloud and reuse the service provider’s front haul/mid haul and the back-haul transport. This deployment option also provides the opportunity to reuse the DC infrastructure of the service provider for compute and store being implemented by the public cloud provider. Critical 5GC management functions and billing/charging functions could be deployed in the telco DC of the service provider network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 244, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '797e2b389fe1574985b3c0a01d1b34a4', 'text': 'Threat Surfaces in 5G MEC Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 244, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '83d30f8131b3c3777f709fe34692ef8e', 'text': 'When the MEC architectural concepts outlined in the previous section are combined into the 5G architecture, the threat surface for 5G expands. The threat surface expands for a number of reasons; among the main ones are the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 244, 'parent\_id': '797e2b389fe1574985b3c0a01d1b34a4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f2a4143aff7d925d675d580570c7ff64', 'text': '• The physical structure of the network is changing, and applications and use cases will require compute and storage locations closer to the edge for reasons of localization and latency. This requires separating certain network functions such as the UPF from the protected perimeter of the service provider’s centralized data center and deploying it closer to the edge of the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 244, 'parent\_id': '797e2b389fe1574985b3c0a01d1b34a4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d7fdc74d2a45aba3010e737248f1612', 'text': '• 5G allows use cases with URLLC to be realized by enabling the third- party applications to be deployed in the MEC. These third-party applications, also called as external Application Functions (AFs), can be integrated to the 5G Core (5GC) network functions using API, with the help of Network Exposure Function (NEF). NEF exposes the 5GC network functions to the external AFs using APIs. These external AFs can also be integrated with other third-party applications using APIs to fulfill requirements of certain use cases, specifically in 5G non-public network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 244, 'parent\_id': '797e2b389fe1574985b3c0a01d1b34a4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '29c5e4235b726f3b3a90dc631b6f7b1c', 'text': '(NPN) industry verticals and enterprise-related deployments. These new API-based deployment options in MEC make API security very important. If API implementation best practices and the right security controls like granular user access controls for APIs are not followed, it will make your MEC deployment risky due to threat vectors related to insecure APIs such as user- and function-level authorization, excessive data exposure, broken object level, and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 245, 'parent\_id': '797e2b389fe1574985b3c0a01d1b34a4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9d539ca82b01677bab461a54ace84040', 'text': '• The structure of the networking functions has changed from physical to virtual implementations, and the functions’ virtualized components can be placed across distributed edge and centralized core clouds. Virtualization, specifically cloud-native functions (CNF), although providing flexibility and scalability for 5G deployments, brings in threat vectors based on the vulnerabilities related to untrusted images, open source software vulnerabilities, improper segmentation, and so on. This makes the MEC more prone to such attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 245, 'parent\_id': '797e2b389fe1574985b3c0a01d1b34a4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '458e785e5ad2471d5ff7e26174cdc382', 'text': '• There is an emphasis on flexible software-based architecture enablers such as SDN, software-defined access (SDA), software-defined radio (SDR), and orchestration to enable use cases related to MEC. Integration of MEC applications with these enablers brings in threat vectors related to improper access control and spinning up rogue virtual instances, among other threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 245, 'parent\_id': '797e2b389fe1574985b3c0a01d1b34a4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '681ff9fb37cc4c47d8c1b185cc6de659', 'text': '• Aside from traditional attacks against servers and caches (for example, via HTTP response splitting), new threat vectors arise. For instance, denial- of-service (DoS) attacks can cause major disruption to the service level agreements (SLAs) committed to by operators. For example, you might have agreed to an SLA with a certain maximum downtime to a content provider who depends on your 5G network to provide content to their customers. In this scenario, because a very large number of caches at the edge of the network would be deployed to cater to a large number of subscribers using low-latency applications (for example, video caching), attackers will be able to easily overwhelm these caches with requests for content not likely to be used by non-malicious users. This situation would result in filling local caches with “useless” content unusable by the subscriber and thereby increasing the downtime period and leading to disrupting the SLA you had agreed upon earlier with the content provider. The vulnerabilities that might cause this to happen would be through traditional attacks on hardware components of the infrastructure,', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 245, 'parent\_id': '797e2b389fe1574985b3c0a01d1b34a4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f40dd1cbad0e5c54c2135b520c7bb3ca', 'text': 'application vulnerabilities, APIs that are not properly secured, and rogue nodes within the architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'parent\_id': '797e2b389fe1574985b3c0a01d1b34a4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '977a109f97d332cb170e7b7ea04e2c75', 'text': 'Figure 5-11 shows an example of threat vectors in 5G MEC deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'parent\_id': '797e2b389fe1574985b3c0a01d1b34a4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '23fcde3772a596c0f6aca3bebf182357', 'text': "Untrusted images Misconfigurations Image vulnerabilities Rogue containers Side-channel attacks CP / UP Sniffing » Malicious VNF / CNF deployment \* DDoS attacks inbound from internet Malicious updates of applications r \* Broken User authentication in API's SP Applications Lateral movement attacks & Internet \* |njection based API attacks e e e e o 0 e 0 e s Improper user access ¢ Data exfiltration Orchestration vulnerabilities e T =X L O% (R ] (Vo) (UPF ] ((A)) j (Cou) (W | R < NI S ~ = MEC Centralized 5GC Improper Access control L] Insecure transport Hardware tampering of Network devices in MEC DC Man-in-the-Middle attacks (MitM) CPU side channel attacks DoS attacks using API vulnerabilities CPU speculative execution attacks « s . Backhaul sniffing Data exfiltration using DRAM / SDRAM hammering attacks ; Physical security on MEC sites (mainly for Enterprise MEC) Improper Segmentation between Enterprise and Service Provider networks", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e739c5b8219610185d625b6e815bd587', 'text': 'Untrusted images', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f796e0ca9b15717160f7ea5d20b5a0d2', 'text': 'Misconfigurations', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6a579c8b64fe66092949c2a0dd8a7674', 'text': 's', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '53eb226ff356c4ca71b5809d4ca9edd1', 'text': 'e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '27b569e6185c7c0e00214a5154fb07ed', 'text': '0', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'parent\_id': '53eb226ff356c4ca71b5809d4ca9edd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '178fef6000a7381d72c154591270cdc4', 'text': 'e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': 'eb35f33b43e977eaf1ce4eff25ed9db5', 'text': '0', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'parent\_id': '178fef6000a7381d72c154591270cdc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'db948640aacbe80c71fcdb16c88cc3f4', 'text': 'o', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '99f5526ac2ec083a0f4bc31cee9f742a', 'text': 'e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '18e9f8b050d896c5b6bf970b6468b06e', 'text': 'e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1e0b308c02aafea5dc176a88a21a462c', 'text': 'e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '39948d6116f4633761c7075a07ff4838', 'text': 'e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1b8c10a433dca09dc55e785a94626212', 'text': 'Figure 5-11 Threats Surface 5G MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'parent\_id': '39948d6116f4633761c7075a07ff4838', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1cb275179600d1aec0b33a189aaf7fcf', 'text': 'As Figure 5-11 illustrates, a wide range of threat vectors exists, depending on the MEC deployment model and the 5G network functions deployed on the MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'parent\_id': '39948d6116f4633761c7075a07ff4838', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'af91c836317d17cf91bf0f8209dbaae3', 'text': 'Physical Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '645b623e0afbd0b70b143f7d53088249', 'text': 'The centralized DC of the service provider or enterprise is usually well-secured with many layers of protection, including physical security layers such as 24×7 manned security. In MEC, the deployment of an edge DC could be in the public cloud or a mini/micro data center with limited space and power resources. A majority of the MEC deployments (even if the hybrid cloud model', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 246, 'parent\_id': 'af91c836317d17cf91bf0f8209dbaae3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7b4235d365970794192d86b15cb23730', 'text': 'is used for MEC) will contain network devices like switches, routers, gateways, firewalls, application delivery systems, virtual workloads such as virtual machines, cloud-native functions, and storage servers. Service providers and enterprises deploying MEC should take stringent measures for securing the site and servers physically. If the MEC site is not physically secure, malicious adversaries might be able to sabotage the site and cause a service outage.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 247, 'parent\_id': 'af91c836317d17cf91bf0f8209dbaae3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e30f4d0e6ad59df9703a6f8defae7ac4', 'text': 'Hardware and Software Vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 247, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7bc8b8a0c4c1898f3cd6d42b7ca79d73', 'text': 'While many of the service providers and enterprises invest in perimeter security such as firewalls and intrusion detection and prevention systems, very few are actually looking at built-in hardware and software hardening. The reality is that if the firmware of the server being used to host all the data center applications is attacked and exploited, it is a very difficult and resource- consuming process to contain the attack and purge all the impacted malicious hosts. Built-in hardening verification is one of the key security checks that should be carried out on the vendor before choosing them as the preferred vendor for MEC (or any data center for that matter).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 247, 'parent\_id': 'e30f4d0e6ad59df9703a6f8defae7ac4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3cafa1c99fdd2ae3508e9df1fa921134', 'text': 'Key areas that impact hardware and software in data centers are malicious software and firmware updates, firmware vulnerabilities, and supply chain vulnerabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 247, 'parent\_id': 'e30f4d0e6ad59df9703a6f8defae7ac4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a8cbd692da9160b00c3f2972bde8855b', 'text': 'MEC sites might also host applications that store user data. The cost of a breach of security can have severe consequences on both the company managing the data center and on the customers whose data is exfiltrated. This makes it very important for you to ensure data loss prevention (DLP) measures, such as monitoring, detecting, and blocking sensitive data while in use, in motion, and at rest, are implemented to adhere to privacy and security laws such as General Data Protection Regulation (GDPR). The GDPR is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations everywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 247, 'parent\_id': 'e30f4d0e6ad59df9703a6f8defae7ac4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3b95e632f0f6af7944d62513466c8aec', 'text': 'Figure 5-12 shows an example of data exfiltration by an attacker deploying a malicious code within a software update.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 247, 'parent\_id': 'e30f4d0e6ad59df9703a6f8defae7ac4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'fc780457aec26bf54683a4913d2329da', 'text': 'o e Tt e it i VNF/ CNF exploited 0 Malicious update Attacker &X. 4¢ ® ‘\_ UPF || MECAppln > I = ® o= = | cu J[ bu |[ Fw |/J e C2C server = Data exfiltration Storage of @ exfitrated data B MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 248, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '303e4c308654ad4abd32e9b0f79a0aaf', 'text': 'Figure 5-12 Example of Data Exfiltration in 5G MEC Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 248, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2fe3fe6148bb56c07bba61358c866d97', 'text': 'As shown in Figure 5-12, the following steps could be used by the attacker to exfiltrate data:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 248, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b1d6ca4a4bf584ed19759933a6c7bd6a', 'text': 'Step 1. The attacker chooses to inject malicious code into one of the updates for the CNF component hosted in the MEC site as the first step.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 248, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '45b8f5904c6674a8d03b3df5754155e4', 'text': 'Step 2. The malicious code that is implanted into the CNF could have a sophisticated method, such as establishing an encrypted layer of communication with the targeted application or host system, as the second step.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 248, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c0fc77f332c197bea501fd8d9d76740e', 'text': 'Step 3. The data can be exfiltrated silently using existing pin holes or open ports in the firewall or by reusing the ports being used for encrypted messages, such as port 443 for TLS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 248, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd3a30c53acfb0021ad0cc69ebeb6fe50', 'text': 'Step 4. This exfiltrated data can then be stored in an external server by the attacker and then sold to other malicious actors looking for stolen data.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 248, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '340635c5f2062cdcaea80b0117009cbc', 'text': 'Figure 5-13 shows an example of data exfiltration by an attacker deploying bugs directly into the chipsets during the manufacturing process, thereby creating a backdoor entry into the hardware server and the infrastructure where the hardware is deployed. If such hardware is deployed in the MEC infrastructure or used by cloud providers in their data center farm where MEC applications are hosted, it can provide a backdoor to the MEC applications and', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 248, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e5420e554a491423fa552ddf6a5bc748', 'text': 'cause mass data exfiltration, or, worse, modification of the data without being noticed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 249, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'dbb0efad51be2735a7c81611476f8f47', 'text': 'Data exfiltration from infected datacenter to C&C o) = o= Destroy data / o= modify data () o Attacker', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 249, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '25a6ee03d97b0e1b6388e387dac9f6d0', 'text': 'PCB design & manufacturing process Chipset Firmware Server assembly and L installation component integration (memory / fans etc.) % vy CSlie ~» = =] il G Server sent for deployment in datacenter server farm / service provider DC / enterprise DC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 249, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7a24e9e693864677950a9699348c1d46', 'text': 'Figure 5-13 Supply Chain Threat Vectors', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 249, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9454e43c0924328fe996a2325dfddfb9', 'text': 'As shown in Figure 5-13, the following steps could be used by the attacker/attacking entity in the supply chain.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 249, 'parent\_id': '7a24e9e693864677950a9699348c1d46', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'text': 'Note', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 249, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2369bf36fc20a8873ef32b1a4ad4d1cf', 'text': 'One of the key differentiators between the supply chain threat vector and other threat vectors is the amount of resource and planning required to pull off an attack. It would also require the support of hardware and software engineering teams of the company manufacturing the chipset and the assembling the server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 249, 'parent\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a6707d2492421487749ab39d7781271', 'text': 'Step 1. The attacking entity could infiltrate the printed circuit board (PCB) manufacturing process and could perform the following actions:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 250, 'parent\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '163edc1fa9f21367f737b65899073271', 'text': 'a. The PCB manufacturing process includes the design phase, which includes the blueprint diagram of the electronic circuit. This blueprint diagram is then used to create tracks on the PCB by computerized systems for mass-manufacturing the PCB boards. The attacking entity can change the schematic to include micro-chipsets for data eavesdropping and sniffing. Another example could be an attack on the BIOS flash memory to modify the hardware configurations.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 250, 'parent\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f7226c5f4983aa769ff7253c0f35408c', 'text': 'b. Once the manufacturing process is completed, the quality assurance (QA) team usually checks the PCB for any anomalies, such as over/under value of voltage, current, impedance of the track within the circuits, and so on. The QA team has to follow certain method of procedure (MoP) documents for the checks. The attacking entity has to ensure that the MoP documents are modified to prevent checks on the malicious chipsets.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 250, 'parent\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '26685e385b70118f8584693e0bdd2ba2', 'text': 'Step 2. The attacking entity could infiltrate the software teams catering for the firmware installation for the chipsets in the PCB.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 250, 'parent\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1a7af2e4608c4e22b36a3371bf2c46dc', 'text': 'The software process includes the firmware coding and installation of firmware on the chipset. The attacking entity could modify the code to add malicious lines of code. The attacking entity could also deploy malicious code during the firmware installation on the chipsets, making the chipsets capable of malicious functions such as overclocking.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 250, 'parent\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fad42385bfb038114e4b44d57ccb9f23', 'text': 'Step 3. The server assembly process is when the PCBs are assembled into the server, along with memory and such.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 250, 'parent\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c9f5fe381f1447e42f554822a7dfde1c', 'text': 'The attacking entity could exploit the memory chips or power controller chips, causing issues when deployed in the data center server farm.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 250, 'parent\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1f0695982d909355a1dcf86da152b5e0', 'text': 'Step 4. The server could then be part of the servers being ordered by the customer, which could be a service provider, cloud provider, or an enterprise.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 250, 'parent\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '39048e81209d0bb46b0bba2fbda6d8a4', 'text': 'Step 5. When deployed in the data center, the server with malicious chipsets and firmware can now create an encrypted connection to the attacker’s', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 250, 'parent\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b216d576f882322d5ca12c5dcd38e300', 'text': 'command and control (C&C) center and cause data exfiltration.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 251, 'parent\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f37c66f7f79e93c4931e6bb0ab5e1d68', 'text': 'Step 6. The malware installed within the server might also be an advanced persistent threat (APT), which might be passive and cause lateral movement within the data center using privilege escalation to look for specific target hosts. Privilege escalation is a method of exploiting a bug or gaining elevated access to the network elements.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 251, 'parent\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd53ac7afbcf90265c79ba9338e3597d4', 'text': 'Step 7. The malware installed within the servers by the attacking entity in the supply chain could also cause wipe-out attacks, destroying sensitive data within the data center.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 251, 'parent\_id': 'b73bfb1d585fee67c778a75ccd79293c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '93e88f635844950012deebc2a82ab084', 'text': '5G MEC Infrastructure and Transport Vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 251, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3ffb4a242bde23d0cceae2af730b9714', 'text': 'Along with major technological change to the mobile packet core and RAN, you will also need to evolve your transport networks to cost-effectively deliver a satisfying mobile broadband experience, while simultaneously meeting the scale requirements for massive IoT and the ultra-low latency requirements for real-time applications. This becomes more complicated when MEC use cases are realized. Depending on the MEC use case and mode of network deployment, the third party MEC applications and the 5GC network functions could be deployed on the public cloud or on the on-premises telco data centers, and the back haul used could be the service provider’s or the public network’s. The MEC infrastructure, be it an on-premises telco cloud deployment, public cloud deployment, or hybrid mode deployment (using both on-premises and cloud infrastructures), should be well secured.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 251, 'parent\_id': '93e88f635844950012deebc2a82ab084', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1af6d14aad15bf648b9118814ffcf657', 'text': 'Figure 5-14 shows an example of the 5G transport traffic traversing through an insecure transport network such as the public Internet.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 251, 'parent\_id': '93e88f635844950012deebc2a82ab084', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '26bed42624d353ba759d78dd92917df6', 'text': 'o SP Services & Internet [ Attacker Insecure Insecure transport transport ( A) [l gNB MEC Centralized 5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 252, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '40435f73b303bdd5f5c8bc800d16326e', 'text': 'Figure 5-14 Attacks Due to Insecure Transport in On-premises 5G MEC Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 252, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '30aa0d1e8cdc5f3a61eea94acff774f0', 'text': 'Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 252, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a439663db3ee1d6e28e595480076ba84', 'text': 'As shown in Figure 5-14, the attacker can sniff the traffic coming into the MEC layer from the insecure public network, and the traffic flowing out to the insecure network is both susceptible to eavesdropping and man-in-the-middle (MitM) attacks. Depending on the applications deployed on the MEC infrastructure, the severity of the eavesdropping could be critical.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 252, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eae2bc6b67e775c3bcf8e60678fce49f', 'text': 'Figure 5-15 shows an example of a transport layer threat vector in the 5G MEC hybrid deployment model.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 252, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ab3a7f7e1bbd35139e552ad93e7f3a60', 'text': ') Appllcanons CU, UPF ttacker 5GCCP (AMF SMF, PCF .. Public cloud deployed Public cloud deployed 5G MEC services core services & Interet = /\\\* NMS, EMS [;j-}é Orchestration Billing v i( R e i E g\\B Front Haul / Mid Haul MEC - Compute & Centralized 5GC storage', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 253, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a639f66a11cf16bd2b3b45e3a78c9f46', 'text': 'Figure 5-15 Attacks Due to Insecure Transport in Hybrid 5G MEC Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 253, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '912e63de07ffaf24e76d0c6cc571f77c', 'text': 'Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 253, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '124b68069cd40cbe04a281b92c2981df', 'text': 'As shown in Figure 5-15, the CU, UPF, and the MEC applications are deployed in the public cloud environment, and the DU, along with compute and storage, is deployed on premises in an edge data center. The interfaces from the on- premises MEC components to the public cloud–deployed network functions, including the MEC applications, are using an API or non-API interface (depending on the application) using the unprotected public network. The communication between the on-premises edge data center and the centralized 5GC is also using the public Internet. Depending on the network functions deployed in the centralized 5GC data center, the mode of communication could be API based or non-API based. In the example shown in Figure 5-15, the network functions deployed in the 5GC are mostly management, billing, and orchestration, which are primarily API based. A majority of the hybrid deployments in discussion plan to have the control plane in the public cloud with the 5GC components handling user-sensitive information being deployed at the on-premises centralized 5GC data center.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 253, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c34ce18bfd6fe750b9ce866115cc0419', 'text': 'The key transport threat vector in the hybrid mode of deployment is due to unprotected traffic while traversing the public cloud. The API communication between the MEC and the public cloud are vulnerable to multiple threat vectors. The 5G MEC API attack vectors are explained in the “5G MEC API Vulnerabilities” section in this chapter. For the non-API communications, some', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 253, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e64798893813d55efe9ce4267a8e8369', 'text': 'of the key threat vectors are eavesdropping and replay attacks, which lead to DoS attacks or theft of sensitive user information.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 254, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '995cc89dc0b675a6d5b66ef4a418eb63', 'text': 'Figure 5-16 shows an example of a transport layer threat vector in the 5G MEC public cloud deployment model.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 254, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '7faf65c76e93af07c10aefa3d459c8a9', 'text': '[ 4 [ ) Attacker CU, UPF e Ly pepuepp MEC application o R e e N L » MEC - Public cloud & Internet ¥ TP -H-- SRR i ) F1 On-premise based virtual DUs ¢---- SRR L SR - —— connected to CU deployed in MEC RU+ DU + MEC hosted in public cloud client RAN site hosted DU & MEC client in least-footprint server', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 254, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '16bd4d901acc01bb97a33532885a398e', 'text': 'Figure 5-16 Attacks Due to Insecure Transport in Hybrid 5G MEC Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 254, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f5e17c654116b494b4987ee9a3de2b7c', 'text': 'Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 254, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1253130a609955dd91719e931fbc2c45', 'text': 'As Figure 5-16 illustrates, in the public cloud deployment model, the CU, UPF, and all control plane network functions are deployed in the cloud. The 5G radio node gNB is co-located with a least-footprint MEC server, which has a virtual instance of DU and MEC clients running on it. This model can typically be used when there is a need to deploy ultra-reliable low-latency communications (URLLC) use cases. The deployment of virtual instances in the low-footprint server in the same location as the gNB allows you to customize the chipset requirements, such as accelerated processing of packets based on hardware', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 254, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '81acca5de944a6706d16a4add9028df7', 'text': 'acceleration as compared to traditional field-programmable gate array (FPGA) chips.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 255, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1caa3f9ba5a98e75e14378045012375c', 'text': 'In this model of deployment, the traffic between the least-footprint servers and the public cloud–hosted 5G network functions are both API and non-API based traffic. The gNB Distributed Unit – user plane (gNB-DU-UP) and the gNB Distributed Unit –control plane (gNB-DU-CP) from the least server hosted MEC toward the CU hosted in the public cloud are non-API-based traffic, while API is used between MEC client hosted on premises and MEC applications/MEC server hosted in the public cloud. Most of the VRAN/O- RAN/C-RAN vendors provide built-in DU-CP IPsec protection, whereas the DU-UP protection is purely optional and depends on the deployment model.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 255, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '97d1a4c57311380f90a2050a71ecdd5a', 'text': 'The key threat surfaces in this model are API vulnerabilities for the on- premises least-footprint server-hosted 5G MEC client interactions with the cloud-deployed MEC applications. Some of the key API threat vectors for this deployment model are improper rate limiting, brute-force attacks, broken authentication, improper configuration of the Docker daemon, and so on. The key threat surfaces in non-API communication, such as between on-premises- based virtual DUs and the cloud-deployed CU is the unprotected DU-UP interface, which is prone to replay attacks, eavesdropping, and MitM-based attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 255, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bfa131424f664745f7c30963bd78e8d1', 'text': 'Figure 5-17 shows an example of a transport layer threat vector in an enterprise-based 5G MEC deployment model.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 255, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '8aee3b0bb2ef9488e0e4ad1f68b9135d', 'text': 'o a To Service Provider RAN / MEC OAM 5G CP functions N2 N4 -— Centralized 5GC N9 Private / Non-Public 5G network DU, CU, UPF connected to centralized 5GC M2M devices (P MEC application control plane functions Enterprise DC Enterprise MEC deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 256, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6c7cff5983e31019ca02744c8fd698ca', 'text': 'Enterprise MEC deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 256, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '400d65de9258dfa7838625faf409fae5', 'text': 'Figure 5-17 Attacks Due to Insecure Transport in Enterprise 5G MEC Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 256, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a53cf67a966f653ced3260fe9d06e5d7', 'text': 'Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 256, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '57e57bebadda707fd89cafd255f3e9b2', 'text': 'In the enterprise 5G MEC deployment model shown in Figure 5-17, the 5G radio network functions, user plane functions, and MEC applications are deployed in the enterprise data center. The centralized 5GC control plane functions are hosted by the service provider. The N2, N4, and N9 interfaces have to traverse through the unprotected public Internet in this example. The details of the interfaces are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 256, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '671d5c19f5a14efdef48e5bc32c208a4', 'text': '• N2: The interface between gNB and AMF in a centralized 5GC or between gNB-CU-CP and AMF', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 256, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '62fabe47cb4d30124fd634c4652e9b68', 'text': '• N4: The interface between the edge UPF and SMF in a centralized 5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 256, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ef8897de004b28f1aa03448e4d056f56', 'text': '• N9: The interface between the edge UPF and UPF in a centralized 5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 256, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c8cf39cfc1f231e322aedd3d454ad781', 'text': 'The key threat vector is the N2, N4, and N9 traffic traversing the unprotected public network toward the 5GC control plane functions and the unprotected API between the MEC applications deployed in the enterprise’s premises and', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 256, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67c19b238a932db8cc7a8e2d3df931b9', 'text': 'the public network. Another key threat is the attacker accessing the service provider’s network functions due to weak segmentation between the enterprise MEC network and the service provider’s centralized network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 257, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cde6794c5001680acc5fa618067b4e1e', 'text': 'Due to the unprotected public network, the N2, N4, and N9 interfaces are vulnerable to eavesdropping, MitM attacks, and reply attacks. The unprotected API interface in the MEC applications is also open to API-related attacks due to security misconfigurations and injection attacks (such as SQL injection attacks) leading to the exposure of sensitive data.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 257, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eafd740fdd7a1ae72bbf845d3a39c9dd', 'text': 'Figure 5-18 shows an example of lateral movement attacks in MEC infrastructures.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 257, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '92ec454804788d8c06e43d37d0be99a2', 'text': 'MEC Centralized 5GC @ EMS O \*5 = 3= . = )/ -— 0 - o', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 257, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c733036804c40bf1e787fe9ff4ee8160', 'text': 'Figure 5-18 Lateral Movement Attack in MEC Infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 257, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2f5d86f9707bb7b80cfdeb8791e8aa69', 'text': 'As shown in Figure 5-18, the attacker infiltrates the network with malicious code or malware, which then moves laterally from the MEC to the centralized 5GC data center. This technique moves deeper into the network, searching for specific sensitive data or a key database of a critical asset. Once the critical asset is found, the malware can then launch a ransomware attack or a wipe attack. Ransomware attack, as the name suggests, is where the malware encrypts the data and then a ransom is negotiated before the files are decrypted. The other malware attack of wiping data is used when the malware finds the sensitive data it is looking for and then wipes it out. There are sophisticated advanced persistent threat (APT) attacks today where the malware even infects the stored data when it is copied from cold storage (archive), thereby infecting each and every copy of the sensitive file.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 257, 'parent\_id': 'c733036804c40bf1e787fe9ff4ee8160', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '65eb440335fd336601e231ee9cc80ae4', 'text': 'The attacker could use the following steps in a lateral movement attack, where the user is an internal employee in your organization:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 258, 'parent\_id': 'c733036804c40bf1e787fe9ff4ee8160', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cdf25d178467ccb68ef0701bb72e200e', 'text': 'Step 1. The attacker infects the laptop of the user with malicious tools for password extraction and malware.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 258, 'parent\_id': 'c733036804c40bf1e787fe9ff4ee8160', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a3caa22e8787bed96609983700f88500', 'text': 'Step 2. The legitimate user uses an infected endpoint unintentionally, such as using the infected laptop to configure the MEC application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 258, 'parent\_id': 'c733036804c40bf1e787fe9ff4ee8160', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '83cf38d7e1cd7dd64528e8ec1741cd6a', 'text': 'Step 3. The malware within the laptop is programmed to steal specific targeted data. A credentials-sniffing tool available in the market today can extract plaintext passwords, hashes, and so on from memory. Once the credentials are sniffed, the malware uses the known credentials to move laterally within the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 258, 'parent\_id': 'c733036804c40bf1e787fe9ff4ee8160', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'be03aedc1bafe89ccff7de6f45f4d613', 'text': 'Step 4. The malware can also move into the 5GC centralized DC using the east-west configuration between data centers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 258, 'parent\_id': 'c733036804c40bf1e787fe9ff4ee8160', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '90f311a63ae68325841b46ab2e465fb1', 'text': 'Step 5. Once the targeted host/data is found, the malware will infect the target. Depending on the type of malware, the attack varies. If the attack is motivated by ransom, then the data within the infected host is encrypted. If the attack is to cripple the network or data, the malware can destroy the data and wipe it out completely.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 258, 'parent\_id': 'c733036804c40bf1e787fe9ff4ee8160', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6d397712b27447206d34ca5d5778798d', 'text': 'One of the reasons the sophisticated lateral attack is difficult to detect is that it can mimic the admin and network traffic behavior. For example, if the admin always logs in around 8 a.m. every day, the malware with the user credentials will also start its activity around 8 a.m. If the network has traffic peaks and reads/writes into the database around 9:30 a.m., the malware will also start modifying the database around that time. This is one of the key aspects of an APT—it is can be passive, understand the network behavior, and then launch the attack, such as a complete data wipe, and remain undetected. A majority of the attacks that include lateral movement and passing malware payloads between multiple hosts also include data exfiltration.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 258, 'parent\_id': 'c733036804c40bf1e787fe9ff4ee8160', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ec6ac451f9e8a4558b0abca3f8487654', 'text': 'Virtualization Threat Vectors', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 258, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '18a5bba1900d4f1ffedb7a790aafeef7', 'text': '5G permits complete programmability and flexibility, allowing the 5G network functions to be deployed as cloud-native functions (CNFs), which are basically container and virtual machine based environments that can be deployed in any infrastructure, such as on a container within the router connected to the radio', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 258, 'parent\_id': 'ec6ac451f9e8a4558b0abca3f8487654', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6d1811f95fa3eb289bf7a86558a40992', 'text': 'node, on an on-premises data center, on an enterprise data center, on a public cloud, or based on a hybrid model of on-premises and public cloud deployments. It brings in true openness in network deployment and implementation of network functions. You can do away with proprietary hardware and software radio and packet core network elements and can use open source software and any commercial off-the-shelf server, or you can use the public cloud to deploy MEC. Although virtualization has been around for a while (since the 1960s), containers based on Docker and orchestrated by Kubernetes are relatively new. In short, while we understand the threats vectors of virtual machines after using them for so many years, we are yet to understand and uncover all the threat vectors of containers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 259, 'parent\_id': 'ec6ac451f9e8a4558b0abca3f8487654', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2006ee6a10c4e544b582eb9812cfa5a5', 'text': 'While virtual environments consisting primarily of virtual machines were prevalent in 4G, they were mainly deployed in centralized data centers secured by a perimeter defense and sometimes deployed in an air-gapped infrastructure. In 5G, the CNF, based mostly on open source programs, is deployed as close to the edge as possible, sometimes even in a multi-cloud stack. This new model of creating network functions with open source programs, having a dynamic runtime environment, and having a new method of deployment will need a serious reexamination into the way security is planned, implemented, operated, and managed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 259, 'parent\_id': 'ec6ac451f9e8a4558b0abca3f8487654', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3ec7fc663b4f38c4e8a1cfc0e18f831b', 'text': 'Typical 5G network deployment will consist of thousands of virtual instances or workloads. If the RAN infrastructure is virtualized, you will have tens of thousands of workloads. While it is good to have virtualization to optimize OPEX/CAPEX and have flexibility of deployment, it does introduce a few new complexities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 259, 'parent\_id': 'ec6ac451f9e8a4558b0abca3f8487654', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4690a0374c2023fb67544d69cfe0a704', 'text': 'One of the complexities is proper segmentation between all these different types of workloads. Previously, before virtualization became more prevalent, the procedure was to interview or talk to people of different departments, such as radio planning, optimization, transport planning, and implementation, and understand who needed what access, what network components needed what kinds of services (DNS and so on), and what traffic needed to exit the infrastructure. The access to specific applications was then planned and configured in the Identity and Access Management (IAM) layer. This method of having manual segmentation/micro-segmentation is inefficient and not scalable for managing tens of thousands of workloads. The solution is to provide micro-segmentation based on rules that can be maintained using behavior analysis of the application. The method for providing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 259, 'parent\_id': 'ec6ac451f9e8a4558b0abca3f8487654', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2f32990ac684367432127c73f806410', 'text': 'automated/semi-automated micro-segmentation is located in the “Securing Virtualized Deployments in 5G MEC” section in this chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 260, 'parent\_id': 'ec6ac451f9e8a4558b0abca3f8487654', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '18caa00fb3277f03e6ab874c054c4820', 'text': 'Another area of importance in 5G MEC virtual deployments is vulnerability assessments. 5G allows open source components to be used to create an MEC application leading to a polyglot microservice architecture. Polyglot generally means that an application developer can use the program language of their choice to create an application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 260, 'parent\_id': 'ec6ac451f9e8a4558b0abca3f8487654', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ceb7685b8f74b90bac6300ad7d8bcaf3', 'text': 'Figure 5-19 shows the polyglot nature of a microservice-based 5G network function or 5G MEC application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 260, 'parent\_id': 'ec6ac451f9e8a4558b0abca3f8487654', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a6f538d06b66de057b584ffdab48d17c', 'text': 'Microservice 1 Container 1 Microservice 5 Microservice 2 (( s Container 2 Microservice 4 Microservice 3 E3 w ((Q Container 4 Container 3', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 260, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0bb73988e9b4163022dc5992eab4ab6c', 'text': 'Figure 5-19 Polyglot Nature of Microservices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 260, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a46151a04966a91b29302db182c2ce47', 'text': 'As shown in Figure 5-19, the microservice is polyglot in nature, which allows MEC application developers to pick a programming language of their choice in order to build products in more efficient ways. In 5G, virtualization of the RAN and 5GC network functions is cloud native based and can be deployed on the cloud. This allows you to use different container deployment models, such as containers on virtual machine, containers on bare metal, or deployed on multiple public cloud. The 4G subsystems might be still deployed on virtual', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 260, 'parent\_id': '0bb73988e9b4163022dc5992eab4ab6c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bd64267a54cab6daccb8c89d52cf4a19', 'text': 'machines (VMs) due to the industry shortcomings on 4G components, but for 5G you might actually skip the container on virtual machine deployment and have it deployed on bare metal or on the public cloud due to the early development of 5G network functions based on containers. For the MEC applications, there have been quite good developments in the containerized space, and there are already applications available today using open source programs that can be deployed in any infrastructure, including cloud. You should be very careful before choosing to deploy any open-source components without validating them for vulnerabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 261, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '27c665aa53adb4f27f71f27f0bd04aed', 'text': 'One of the key issues is the lack of visibility in checking if any of the programs has a vulnerability that needs to be patched, as shown in Figure 5-20. If it’s only one microservice that needs attention, it can be checked and updated manually. But in 5G, when we have tens of thousands of MEC applications, it becomes very difficult to conduct a vulnerability assessment and compliancy check.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 261, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '820a04ede962f8ffa67a9404fe24a3f8', 'text': 'MEC hosted in Public cloud A 1] I %‘ll‘ ‘. 4 in open-source CNFs II’ [ | ] [ [ ] A) i ll;<\_. i < > Centralized 5GC RAN-Site Iow - i iii"\' R footprint MEC Z On-premises \\ I’-Q— Enterprise deployed MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 261, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6a558f22b09aa1509346234948809051', 'text': 'Figure 5-20 Vulnerabilities in Open Source Cloud-Native Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 261, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '51ad0a7b05e62cd61ef575ad31b603a5', 'text': 'As shown in Figure 5-20, it becomes really tricky if you need to have a visibility into the vulnerabilities of all open source programs across the entire stack of MEC deployments, whether deployed in a multi-stack cloud, RAN site low-footprint MEC, on-premises MEC, or enterprise-deployed MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 262, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '098f1a92b6178cb8927c07a4bd36d15a', 'text': 'Attackers are constantly innovating methods to exploit the container ecosystem in order to exploit the vulnerabilities/improper configurations to launch attacks. Docker is one of the most widely used platforms for managing containers. Over time, it became the de facto standard for development and deployment of web and cloud applications; however, anybody who has worked with Docker quickly realizes that the learning curve is quite steep. Therefore, Docker installations can be easily misconfigured and the Docker daemon exposed to external networks with a minimal level of security.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 262, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '95d30701feb8259160503690340fb697', 'text': 'Figure 5-21 shows crypto-mining malware spreading through the system via an attacker exploiting an incorrectly configured Docker API for third-party MEC applications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 262, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'bade7dccb0d6f57322aa433e243ee0d1', 'text': 'o= = a = Attacker C2C server Credentials discovery & Crypto mining Infecting Docker container images within the Docker hub repository using open APl port - i 5G MEC application downloads the infected Docker container images from the Docker hub n-premises Z0 EC \_- ( A)) > %‘f (TR On-premises Centralized MEC 5GC | ? | Malware lateral movement between MEC sites', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 263, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2c89c98c5bb78a6035daff369c4c42b8', 'text': 'Figure 5-21 Attacker Exploiting an Incorrectly Configured Docker API', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 263, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '38a8b75051a569a1587fdfd3105dd912', 'text': 'As shown in Figure 5-21, the main threat vector here is an incorrect configuration of the Docker API, which is exploited by the attacker to gain access to the system that hosts the third-party 5G MEC application. The attacker then laterally travels into another MEC site, a centralized 5GC site, infecting other systems and using it for crypto-jacking (stealing credentials and other sensitive data). For the sample attack shown in the Figure 5-21, the steps are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 263, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67657eb0317c7a82df0a82f01a038018', 'text': 'Step 1. The attackers scan the Internet for Docker containers implemented with an unprotected or incorrectly configured API. In case of Docker, the Docker daemon listens for API requests and also manages Docker objects, such as images, containers, networks and volumes.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 263, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd7a2dd09532e4678f06360e5fcc8a664', 'text': 'Figure 5-22 shows the Docker architecture and the API the attackers are trying to exploit.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 264, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '25ad246d24b2cc8734d28d6549cbdae2', 'text': 'APl which the attackers try to exploit Containers Images', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 264, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd7af7d3998ce2885fe65d3590e597015', 'text': 'Figure 5-22 Docker Architecture and the API That Attackers Try to Exploit', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 264, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9d40e67ad1784a745579a53f2fc8901c', 'text': 'Step 2. This infected image is pulled and run as containers on the compromised host. This can be easily accomplished if there is malware already present in the MEC host causing a privilege escalation attack.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 264, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '925fdc031f6ff7ffe9c0a48e32a18e9b', 'text': 'Step 3. The infected code within the container can also cause the malware to spread deeper within the local and remote networks. The main module could also attempt to spread to other hosts by stealing the client-side certificates and connecting to them without requiring a password. The other modules within the infected container image can also include scripts for actions such as terminating security services such as anti- malware solutions and removing a competitor’s botnets. It can also be programmed to protect itself and hide the mining process from process enumeration tools.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 264, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '04b9edca57c16303fb5858757780e479', 'text': 'Step 4. Once ready, the scripts within the infected container image can now extract sensitive information, such as number of CPUs and user credentials, to the C2 server, which can now be used for calculating the mining capabilities. The crypto-jacking worm can now be used for', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 264, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fe62c303fa8484367f5f3984dcb8781c', 'text': 'mining. The infected container image can query the C2 server for other hosts it can infect.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 265, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2b9bd9f955fbc0829f81dabc08b4ae24', 'text': 'Among other threats linked to virtualized deployments, the side-channel threat vector is quite important because it can impact any virtual function sharing CPU memory. There are many variants of side-channel attacks, such as hyper- jacking, Spectre, Meltdown, Cross-VM cache side-channel attacks, and so on. These are generally aimed at leaking the crypto keys, which are then used for eavesdropping or exfiltrating the data out of the infrastructure. Cross-VM cache side-channel attacks are well-planned sophisticated attacks focused on a particular organization. The side-channel attack method chosen by the attacker depends on many factors of the target network implementation, such as installed MEC infrastructure components, the vendor and model of chipsets being used in the MEC data center, the type of network devices present in the targeted MEC network, and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 265, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '694ae16f866572dcc377ebcc3cdf797c', 'text': 'Figure 5-23 shows an example of data exfiltration due to CPU processes used in virtualization.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 265, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c16cd49715c306585d27c2c8936db6e9', 'text': 'e MEC application Attack CNF2 VNF 2 E A ? o= oo EEEE \_\_\_\_\_\_\_\_\_\_\_ =y~ S \_ by e F--p o= == = = C2C server Storage server E ! —» ‘.. MEC server p¥ e MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 265, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7daacd86d6bc2d5896bc6c61947055f3', 'text': 'Figure 5-23 Data Exfiltration Due to Side-Channel Attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 265, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0c883c36a42b9bb5229ea61a1b10d626', 'text': 'As shown in Figure 5-23, which shows the attack vector aimed at the virtualization infrastructure’s firmware, the attacker can use the following steps:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 265, 'parent\_id': '7daacd86d6bc2d5896bc6c61947055f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '76198dadf2e913cf233a017b494e6c0b', 'text': 'Step 1. The attacker uses side-channel attack vectors such as a cross-VM cache side-channel attack and utilizes the underlying hardware CPU vulnerabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 266, 'parent\_id': '7daacd86d6bc2d5896bc6c61947055f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a8056549039a449a7650f6fe537e6335', 'text': 'Step 2. The attacker’s side-channel attack vector allows one process to extract sensitive information by exploiting shared cache memory between VMs and analyzing the data, such as the relation between the software process and the power consumption of the hardware for that process.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 266, 'parent\_id': '7daacd86d6bc2d5896bc6c61947055f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0f3d417c8439fe3a5f5e84d791e65fc3', 'text': 'Step 3. The data can be exfiltrated silently using existing pin holes or open ports in the firewall or by reusing the ports being used for encrypted messages, such as port 443 for TLS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 266, 'parent\_id': '7daacd86d6bc2d5896bc6c61947055f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a3fab24e58616e018a8190e52d10ff07', 'text': 'Step 4. The exfiltrated data is analyzed to understand the software process and the type of software being used, among other things. Once the software is understood, it can be used to launch a crippling attack at a later stage.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 266, 'parent\_id': '7daacd86d6bc2d5896bc6c61947055f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '24dd2c86ca981c7797b40fd1a0baa621', 'text': '5G MEC API Vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 266, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '80e6a8c872028996bfef279758bf7588', 'text': '5G architecture has been designed to be cloud native, as it brings elasticity, scalability and creation of rich services in the edge. 5G also allows you to expose rich services through the cloud and RESTful APIs. APIs make it very easy to integrate between different solutions and information sharing to enable a seamless user experience. API introduction for MEC applications also brings in the expertise of web application developers in developing 5G MEC applications, but it also brings in new threat vectors.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 266, 'parent\_id': '24dd2c86ca981c7797b40fd1a0baa621', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b0f7c5aaef51ec40ef5e36fc6a353823', 'text': 'Figure 5-24 shows an example of API threat vectors in 5G MEC deployments, where the attacker uses an injection attack causing DoS to the devices being served by the MEC applications hosted on the MEC server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 266, 'parent\_id': '24dd2c86ca981c7797b40fd1a0baa621', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '162798aff8fdff0467446a36ab186732', 'text': ', MEC Applications [} [ Service CM Service PM ¢ D ¢ Pod Pod € App App API TR T >3 Gateway e e e ] Service Service FM Analytics Attacker Pod " pod | App App MEC hosted on Public or Private cloud of Enterprise or Service Provider', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 267, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6bd9e8c280fe5d67ffcc008a197b3a15', 'text': 'MEC hosted on Public or Private cloud of Enterprise or Service Provider', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 267, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bc9fbb2d897a9b46a361bb88c86d0b24', 'text': 'Figure 5-24 API Injection Attack in Applications Deployed in MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 267, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '06bd2dbdf3dad6f6164d1b1a47c07c13', 'text': 'As shown in Figure 5-24, the attacker uses an injection attack, which occurs as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 267, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cce10ea5f6e01df22f06f3939c3f85de', 'text': 'Step 1. The attacker gains control of a weak IoT device and gets the credentials of the target server to be exploited.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 267, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '845f75853eb5e2ff7eeb3eea4cf728d7', 'text': 'Step 2. The attacker constructs API calls that include command injection, NoSQL, and so on, toward the CM server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 267, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '63fcee32f74ff2c9a2e438a57b3916d0', 'text': 'Step 3. The API gateway does not perform any checks and passes the calls to the CM server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 267, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '59c52645acf19a872c933b7ea5e1751d', 'text': 'Step 4. The CM server blindly executes the calls, which will crash the CM server, causing DoS to all the devices being served by the CM server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 267, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e882952eac8400040e34d37b38913b3a', 'text': 'In this threat vector, the attacker is hidden completely and uses the existing device to launch an attack toward the MEC. This attack could be launched directly by the attacker using the API.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 267, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd0543b9d774faf43a76746b367cb009a', 'text': 'Figure 5-25 shows an example of API excessive data exposure attack.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 267, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '7cd4a57cf7408409c1fdcbc6f0e8baa2', 'text': 'MEC hosted on Public or Private cloud of Centralized 5GC hosted on Public or Private Enterprise or Service Provider cloud of Enterprise or Service Provider / Config data - \* Storage / Cache \* M2M device mventory E\\ @ wwww @ UPF API Gateway ® Raw data collected from the M2M application database by the attacker [ Att éer® k', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 268, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b3b3c3abe23701ddd839942d020ff9a7', 'text': 'Figure 5-25 API Excessive Data Exposure Attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 268, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2c7c0736a9051deeb0434f0eee5c3414', 'text': 'As shown in Figure 5-25, the attacker uses an unprotected API to gain excessive data exposure from the configuration management. In one of the attack vectors, the following steps could be used by the attacker:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 268, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36f902f450cc090c2035b5859bca9da0', 'text': 'Step 1. The attacker requests data using “API Get” toward the API gateway.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 268, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '71f3f8579b1806420b58b827b814ad07', 'text': 'Step 2. The API gateway relies on the client to do the filtering.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 268, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eda453bf9a7dd39870b5c72072731574', 'text': 'Step 3. The API gateway passes the query to the database. Depending on the data requested by the API Get request, the request could also be forwarded to the 5GC CP objects using NEF (Network Exposure Function). The NEF can see the request coming from the MEC applications as a legitimate request, which in turn can respond with the attribute values/bulk configs requested by these API calls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 268, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '77630cce7a830a2e43a07114ec11a9f0', 'text': 'Step 4. The API returns full data objects as stored in the M2M application database. Depending on the data requested by the API Get request, the data could also be purged from the 5G CP objects using the Network Exposure Function (NEF) API calls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 268, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '389f2e35befb31d20131f40348fec038', 'text': 'Step 5. The attacker collects all the information, which might include sensitive data such as device IDs, Day 0 configuration templates, username and passwords, and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 269, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '968eb47e85454383fc18109dbac03e22', 'text': 'Figure 5-26 shows an example of excessive data that can be exposed if filtering polices are not used on the MEC application server side.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 269, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '33a5aaf8e401508c51d48bed55ffa674', 'text': 'MEC application hosted on Public or Private cloud of Enterprise or Service Provider', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 269, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd1a3193e874a82e006d5e5ea7636647e', 'text': 'MEC application hosted on Public or Private cloud of Enterprise or Service Provider \* Config data - ¢ Storage / Cache N ¢ M2M device inventory MEC database retums all altribute - value pairs ~ . l 4—> N N N ToNEF ] ‘devicename”: devicel ‘deviceid": 1025a16d771cc6197fd GET request to / deviceidinfo device1 ‘power output™ 10mW ip address”:10.10.10.11 ‘address":1 Main street, Swords, Dublin ‘username”.abcd @hotmail.com ‘password":"abed1111" . AP Gat y Excessive data retumed and ‘devicename": device110 GET request to /deviceidinfo device1 no filtering policy used by service provider / enterprise ‘deviceid": 7f31a74d113fc192df1d ‘power output™ 10mW in MEC server end ip address™:10.10.10.111 ot e ‘address": 1 seatown, Swords, Dublin ; sername":abed @hotmail.com User / ‘password""abed1211 attacker & oA', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 269, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'eb12bcf092cd6e8883fadea71b286f68', 'text': 'Figure 5-26 API Excessive Data Exposure Attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 269, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6fbf7f0afc64b6afd73b064813056b84', 'text': 'As shown in Figure 5-26, the excessive data can be obtained by the user or an attacker. This attack, aimed at getting sensitive data out of an MEC application database, can cripple industry verticals such as smart cities and smart manufacturing and is very critical for defense and military use cases. The threat vector here is due to the weak security controls, where the API exposes a lot more data than the client requires and relies on the client to do the filtering.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 269, 'parent\_id': 'eb12bcf092cd6e8883fadea71b286f68', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ccd6e10237f27ac63bd2366a826b5b0e', 'text': 'Figure 5-27 shows an example of Broken Object Level authorization and Broken Authentication API attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 270, 'parent\_id': 'eb12bcf092cd6e8883fadea71b286f68', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f94510f60d63ad5ed0211c354f0f7425', 'text': 'MEC hosted on Public or Private cloud of Enterprise or Service Provider = 0 MEC application @ user & admin . database Admin Legitimate adm|n user from enterprise A/\\ cannot log in = \\/ To 5GC NEF component « L MEC Application J ) 2)| v API Gateway Change attribute for certain admin users (4 AN v U = J All user info and credentials 9 downloaded Attacker', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 270, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'def5ccca24c856f577b40e19771b9ea7', 'text': 'Figure 5-27 Broken Object Level Authorization and Broken Authentication API Attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 270, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c8dd99e69a2c7a79218bc80f0209b7b3', 'text': 'As shown in Figure 5-27, the attacker uses Broken Object Level authorization and Broken Authentication to attack the application deployed in the MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 270, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f369e9b92374b351c88dda47e505c688', 'text': 'The following steps could be used by the attacker:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 270, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1a4ea2eed1011adb46c08829cbf40b13', 'text': 'Step 1. The attacker sends an API call with the admin-level APIs requesting all user information from the database. For example, instead of using /api/users/MEC\_application/user/my\_personal\_info the attacker could use /api/admins/MEC\_application/users/all\_personal\_info', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 270, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd1758bdfe17cd83baebff7b410c1d112', 'text': 'Step 2. The API gateway relies on the client/user to use a user-level or admin- level API, and hence the request is seen as a valid request from a client/user.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 270, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '829c458f99d58d1018da176e9be0b3b3', 'text': 'Step 3. The database responds to the API call with all user information, which might include PII (personally identifiable information), which is the personal data of all the users using the application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 271, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3a66af7ab10e9c19946466ae85442156', 'text': 'Step 4. This information is collected and analyzed by the attacker.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 271, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '163e7b20ed8805970763ed0eea2c7d3d', 'text': 'Step 5. The attacker can now use the ID of another user and launch an attack toward the MEC application user and admin database and remove the admin users.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 271, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '34ca2c5bb84d14b13ef3c44918d6beb0', 'text': 'Step 6. The legitimate admin users cannot access the MEC application and are denied any service.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 271, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '77e6630abf8b060a9c7ced3edbe52291', 'text': 'This attack can have multiple critical impacts on the service provided by the MEC application and its users. The attack also prevents the administrators from accessing the MEC network, and hence the network or service outage can extend to a longer period of time.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 271, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '288683c0047aa879a35a52e58cb5c7f5', 'text': 'DDoS Attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 271, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '78e533da1737327b19316e17a7c18306', 'text': '5G use cases, as mentioned in the previous section, will change the way computing elements and IT services are deployed, and this includes application deployment, which is virtualized and highly distributed to enable ultra-reliable low-latency communication (URLLC) use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 271, 'parent\_id': '288683c0047aa879a35a52e58cb5c7f5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0f6bac647181259fc7fbe0663220d01b', 'text': 'One of the key DDoS threat vectors that’s very specific to 5G is the zero-day DDoS attack. The main reason behind this is that it’s the first time in the standards that cloud-native architecture has been mandated for a 3GPP technology, and that technology is 5G. The network functions in 5G are based on cloud-native technology, which relies on open source software components and open interfaces. When the service providers and enterprises adopting 5G use these open source components and open interfaces, such as REST API methods, the developers will follow suit, and the MEC applications developed by various third-party and inhouse software developers will all use the same open source components and open interfaces so that all the 5G network functions and the third-party MEC applications can co-exist in the same environment. This is the first time in any 3GPP standard so far that such openness and flexibility are allowed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 271, 'parent\_id': '288683c0047aa879a35a52e58cb5c7f5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '63a75255de588e3c70a4336a37b21dcb', 'text': 'This new application deployment method using open source components and cloud-native-based architecture also brings in threat vectors like zero-day DDoS attacks, which will consist of new attacks based on the vulnerabilities of', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 271, 'parent\_id': '288683c0047aa879a35a52e58cb5c7f5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '66d3ae5d572158eb1f6f2f6e4122c48e', 'text': 'these open virtualized environments where the patches have not been created yet or are not yet available. Once the vulnerabilities are known by an attacker or a group of attackers, they can be traded among malicious individuals who can be sponsored to take down the critical infrastructure of service providers, enterprises, or even critical security services deployed by the country to protect important government infrastructures. In this section, we will look at the 5G- specific DDoS attacks to better understand the actual threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 272, 'parent\_id': '288683c0047aa879a35a52e58cb5c7f5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aec3e4106c9fa51ed0cf3045f1aa1533', 'text': 'Figure 5-28 shows an example of inbound DDoS attacks from the Internet using container/image vulnerabilities and causing a DoS in a 5G MEC deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 272, 'parent\_id': '288683c0047aa879a35a52e58cb5c7f5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '6e2a21e909b2731475975a7db21dd3cb', 'text': '[ : a ", MEC Attacker 208 Application Internet / Public cloud % 4 MEC services deployed in public cloud a4 - el ((A>) , , i( = \\1 A gN\\NB WL Devices using MEC MEC - Compute & application storage', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 272, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5910014f7e377f171349b66c57192844', 'text': 'Figure 5-28 Inbound DDoS Attack in 5G MEC Components Deployed in Public Cloud', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 272, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '664aa838a37c949f414b0b455d872d92', 'text': 'As shown in Figure 5-28, the attacker causes inbound attacks on the applications deployed on the public cloud MEC layer, leading to the DoS to legitimate users of MEC application. These attacks could also be a type of zero-day attack.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 272, 'parent\_id': '5910014f7e377f171349b66c57192844', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '88cbd9d58c05a642f300ac5e41144186', 'text': 'The following steps could be used by the attacker:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 273, 'parent\_id': '5910014f7e377f171349b66c57192844', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7d492798f8588ab91b0b29f7fdb8c041', 'text': 'Step 1. The attacker scans cloud repositories for unprotected images or a runtime environment. Cloud repositories are where people share container images. Some of the commonly used cloud repositories also allow people to create, manage, and deliver container applications and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 273, 'parent\_id': '5910014f7e377f171349b66c57192844', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '46f714e30ba12d4606bbe6fb5df2f783', 'text': 'Step 2. The unprotected runtime environment could then be assigned malicious code by the attacker. The attacker could then build an image using the runtime environment and upload it into the cloud repository and then start running it. As per the modified command string or the assigned malicious code, the images then start infecting other open and unprotected daemons to create a botnet.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 273, 'parent\_id': '5910014f7e377f171349b66c57192844', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a8d22863ba613b3802a94f3ae5dfa87e', 'text': 'Step 3. The botnets are all assigned a specific target host (MEC application deployed in the public cloud) to attack.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 273, 'parent\_id': '5910014f7e377f171349b66c57192844', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b5ef7b6c37467e3ee895f4a2f51fdb77', 'text': 'Step 4. The targeted host (MEC application) is under DDoS attack. Depending on various DDoS methods, the MEC application would be busy processing the request or artificial consumption of bandwidth by fully utilizing the maximum number of concurrent sessions possible.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 273, 'parent\_id': '5910014f7e377f171349b66c57192844', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a42cb942738fb47fe194188dc9972d28', 'text': 'Step 5. The MEC application cannot respond to legitimate users or use cases, thereby causing network outage or DoS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 273, 'parent\_id': '5910014f7e377f171349b66c57192844', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '63c514023b4c61340ba8586ff9b86d49', 'text': 'Figure 5-29 shows an example of inbound DDoS attacks from the Internet using and causing DoS in a 5G MEC deployment for legitimate requests.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 273, 'parent\_id': '5910014f7e377f171349b66c57192844', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '65be058850125a12987964123f99903b', 'text': '+“—> O Attacker SP Applications & Internet [N DDoS and Legitimate inbound traffic from Internet ® i i 0% DDoS attack takes down the MEC application / MEC service e ]+ causing service outage A A To 5GC NEF component v v e e UPF MEC application DB /', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 274, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6fc69bf02183836e600d46060514977f', 'text': 'Figure 5-29 Inbound DDoS Attack on MEC Applications Deployed in an On-premises MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 274, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd8d8c41debb57defcf4bf2e2f35151ea', 'text': 'As shown in Figure 5-29, the attacker creates an artificial exhaustion of resources and prevents legitimate requests to be processed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 274, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '68b8f9a4487a7ecd4420e0a38bc97ed9', 'text': 'The following steps could be used by the attacker:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 274, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a23b0802111af7b12ca6fa4bd9e929ce', 'text': 'Step 1. The attacker exploits the cloud-based open source programs using existing vulnerabilities and turn them into bots. These bots, in turn, scan for any other similar vulnerable programs deployed in the cloud, such as in cloud-based repositories, and turn them into bots.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 274, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5dc33ef58c5950d00b7b2f4dcf027e88', 'text': 'Step 2. Once the botnet has been established, the attacker is able to orchestrate an attack by issuing remote instructions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 274, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '784c2f33522004177d6d6922a13f6004', 'text': 'Step 3. The MEC application server becomes overwhelmed by the number of requests, preventing it from processing legitimate requests and thereby causing DoS for legitimate requests.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 274, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '04ff849d55514a15d273e5111e59f38c', 'text': 'Figure 5-30 shows an example of DDoS attacks caused by lack of resources and rate-limiting thresholds on the API calls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 274, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'cca2a11cd70a584ae334760bfec86cd7', 'text': 'UPF ~(lK MEC Application » To 5GC NEF component —— ! . AP| Gateway [ 4 DDoS -e;ttack from devices being served A by MEC applications —» » | \\ \\ r{” | — \\ | | "““‘m \\ x- e w p w x A x w', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 275, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '13cd3da58bb8cd59654a91d8a52db06e', 'text': 'Figure 5-30 DDoS Attacks Due to Improper Rate Limiting on APIs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 275, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '856a8386ffb3fe69a3d63fc2bbf177e4', 'text': 'As shown in Figure 5-30, an attack could be initiated by directing a large volume of devices toward the MEC infrastructure hosting the MEC application serving the devices/users. This attack vector can be seen as an application layer attack, as it includes GET/POST floods and targets the vulnerabilities of the API and/or the operating system. These threat vectors are aimed at taking down the servers and causing DoS, and when aimed at critical services and government infrastructure, they can lead to very challenging situations.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 275, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '725a7a56038cc690ebacde6cacf9a651', 'text': 'Usually, these types of API communications are based on the devices reaching out to the MEC applications or certain network functions such as functions catering for real-time analysis behind the API gateway for use cases such as uploading certain values and getting certain attributes modified by the configuration management of the MEC applications. If these APIs are not', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 275, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b31a90d64e9f279a962222964cbaaa3e', 'text': 'protected by rate limitation and payload size, the threat vectors, such as an excessive amount of API calls causing DDoS, can take place, causing DoS to the legitimate API calls from devices. These unprotected APIs can also allow brute-force attacks, which can take down the MEC applications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 276, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3d3c81fbddf7c6cc35289db15f83b650', 'text': 'Securing 5G MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 276, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '89a1275e2ca73c959b3cf1f2111c9a87', 'text': '5G edge deployments will supply virtualized, on-demand resources with an infrastructure that connects servers to mobile devices, to the Internet, to the other edge resources, and operational control system for management and orchestration. These deployments should have the right security mechanisms in the back haul to prevent rogue deployments and the proper security controls to prevent malicious code deployments and unauthorized access. As these MEC deployments will include the dynamic virtualized environments, securing these workloads will be critical. Securing transport, SDN, and orchestration will ensure that service providers are able to provide their services securely from the edge of the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 276, 'parent\_id': '3d3c81fbddf7c6cc35289db15f83b650', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '507cb7a02bc257a35ce10ef84c91cca1', 'text': 'Physical Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 276, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e6117953e92c7fab8f593b5ff396976d', 'text': 'Security teams must prepare for new threats that emerge with little to no warning. Part of the solution to this problem lies in technology. It is increasingly common to include the ability to detect and mitigate attacks on various devices, including routers, switches, security appliances, and end hosts. Proper device hardening and the use of security features on these devices can go a long way toward stopping a major outbreak before it occurs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 276, 'parent\_id': '507cb7a02bc257a35ce10ef84c91cca1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f5df0adfb0425e562bfb8d3143aaf7ae', 'text': 'MEC enables the deployment of containerized 5G network functions in locations closer to the user. Locations closer to the user include on-premises data centers (DCs) of varying footprint and public multi-cloud deployments. Apart from public cloud deployments of MEC, the on-premises deployment of a data center would require layered physical security to ensure that the MEC is secured. Physical security is more critical in an enterprise DC, where the 5G network functions and MEC applications might be deployed in the same DC as the enterprise applications. Some of the key physical security measures are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 276, 'parent\_id': '507cb7a02bc257a35ce10ef84c91cca1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '52aae5cf8c5c00211fd422cdabbb6dda', 'text': '• Monitoring: One of the key elements is to avert the attacker and prevent any unauthorized entry into the premises. Having a visible CCTV camera,', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 276, 'parent\_id': '507cb7a02bc257a35ce10ef84c91cca1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '63114f2df539288c87d8996e470dd691', 'text': 'signboards, drone surveillance, automatic light based on motion detection, and so on might ward off an attacker, causing them to look for less- protected areas. The monitoring system should have a cold storage method of housing the recorded surveillance.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 277, 'parent\_id': '507cb7a02bc257a35ce10ef84c91cca1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d4f58d82ae93f6af81fc0d4180fcd37', 'text': '• Access controls: MEC DCs should include access control systems using card swipes or biometrics. High-resolution video surveillance and analytics can identify the person entering and also prevent tailgating. Video surveillance should also be able to read license plates and conduct facial recognition. You should use multiple different techniques to provide multiple security layers and restrict unauthorized entry.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 277, 'parent\_id': '507cb7a02bc257a35ce10ef84c91cca1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5dababdca3a1275d41a08f4727aa53ca', 'text': 'Here are some of the key best practices for physically securing the on-premises MEC data center:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 277, 'parent\_id': '507cb7a02bc257a35ce10ef84c91cca1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '88ef6c6401db4c9528c77da0a18be840', 'text': '• Access controls for the data center should have multiverification options, such as access card/biometric/fingerprint to provide an extra layer of security.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 277, 'parent\_id': '507cb7a02bc257a35ce10ef84c91cca1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e9195e93a5b6ec759f6fb5b08a71fcd6', 'text': '• Audit mechanisms and tools should be in place to verify policy enforcement and to determine how data is stored, protected, and used, to validate service.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 277, 'parent\_id': '507cb7a02bc257a35ce10ef84c91cca1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1349ed1f11a89d446df45adb71abd722', 'text': '• Internal audits should be carried out regularly to check for any vulnerabilities in the process for access as well as to ensure proper working of the CCTV cameras and related storage of the captured camera footage.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 277, 'parent\_id': '507cb7a02bc257a35ce10ef84c91cca1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e37d8c717702f970d96c581b02c619aa', 'text': '• Risk management programs should be in place to deal with the continuously evolving deployment modes of MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 277, 'parent\_id': '507cb7a02bc257a35ce10ef84c91cca1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0c85a73d52a4218907b5f872daf1f840', 'text': '• Access controls should be regularly checked and updated to reflect the changes in the job roles of the personnel accessing the data center.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 277, 'parent\_id': '507cb7a02bc257a35ce10ef84c91cca1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '04b5c3406caf8c4158ac8417e0078559', 'text': 'Hardening Hardware and Software', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 277, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '760a6f669b5309d40cc00cd81eeb7510', 'text': 'Being cloud native and completely software driven, 5G uses open source technologies. Although this is critical for scalability and allowing cloud deployment integrations, vulnerabilities from multiple open source applications could be exploited by attackers. To reduce the attack surface, you need to verify the 5G vendor-specific secure development process to ensure hardened software and hardware. Vendors should follow the secure development', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 277, 'parent\_id': '04b5c3406caf8c4158ac8417e0078559', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b941f377dad31fee7c32c13e7640069b', 'text': 'lifecycle (SDL) process, adhering to standards such as ISO27034 and ISO9000 for compliance requirements. ISO27034 provides an internationally recognized standard for application security, while ISO9000 helps ensure you meet the statutory and regulatory requirements. One way of doing this is to ensure that you choose vendors that have undergone testing for Federal Information Processing Standard (FIPS) compliance. This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing qualitative levels of security intended to cover a wide range of potential applications and environments. Level 1 provides the lowest level of security, while Level 4 provides the highest level of security. The security requirements cover areas related to the secure design and implementation of a cryptographic module. The public cloud providers for 5G MEC should be authorized by FedRAMP.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 278, 'parent\_id': '04b5c3406caf8c4158ac8417e0078559', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '630795763eabdd2e2de35d49caf76d63', 'text': 'FedRAMP is a U.S. government program to standardize how the Federal Information Security Management Act (FISMA) applies to cloud computing services. FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring of cloud-based services. Using a “do once, use many times” framework, FedRAMP reduces the cost of FISMA compliance and enables government entities to secure government data and detect cybersecurity vulnerabilities at unprecedented speeds.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 278, 'parent\_id': '04b5c3406caf8c4158ac8417e0078559', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ae6aa652d9d18a8ce40fcbffd9da82c2', 'text': 'FedRAMP was developed in collaboration with the National Institute of Standards and Technology (NIST), General Services Administration (GSA), Department of Defense (DOD), and Department of Homeland Security (DHS). Other government agencies, working groups, and industry experts participated in providing input into the development of FedRAMP. It was launched in 2011, with the main aim to promote the adoption of secure cloud services across federal agencies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 278, 'parent\_id': '04b5c3406caf8c4158ac8417e0078559', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2987216f806da20e67f1fbf60882af25', 'text': 'FedRAMP assessment is quite stringent and takes around 6 to 9 months to complete, and the certification is valid for 1 year. While not all solutions that have achieved FedRAMP authorization might be available for public consumption, by selecting vendors that have achieved FedRAMP authorization on cloud solutions for 5G deployments, you will be taking a step in the right direction.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 278, 'parent\_id': '04b5c3406caf8c4158ac8417e0078559', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '115d17d44fe43c26a337e9a4d9233928', 'text': 'Just choosing vendors having a robust SDL process and following standards for hardened platforms is not enough to ensure you have a hardened system in place. SDL, in fact, is a continuous journey, as you ensure the secure process is', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 278, 'parent\_id': '04b5c3406caf8c4158ac8417e0078559', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ead04bf1695746a0c47b47607612c10c', 'text': 'catered for during design, initial deployment, software updates, hardware upgrades, maintenance, and migration.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 279, 'parent\_id': '04b5c3406caf8c4158ac8417e0078559', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6a64b4029096b971244d6a0aaa01c816', 'text': 'The first step in having a hardened process is to have a secure boot process where the OS boot images are authenticated against a hardware root of trust. Having the secure boot process authenticating against the hardware root of trust makes it very difficult for an attacker to cause tampering attacks and expose the encryption keys. Without the hardware root of trust, third parties can tamper with BIOS, boot loader, or ROM monitor (ROMMON) boot code to load modified software images; bypass hardware, authenticity, and licensing checks; or perform additional functions with malicious intent. Tampered code can also result in data manipulation or data theft, and it can provide a platform to launch attacks, including DoS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 279, 'parent\_id': '04b5c3406caf8c4158ac8417e0078559', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4763a4756bc9530de1c775d21044a6dd', 'text': 'Hardware root of trust is provided by many vendors by using the Trusted Platform Module (TPM), also known as ISO/IEC 11889. TPM was conceived by the Trusted Computing Group (TCG). The primary scope of TPM is to ensure integrity of the platform. This section primarily details the hardening of the MEC infrastructure. Using embedded security within the MEC servers will help protect the keys, passwords, and digital certificates. One of the key advantages of TPM is the ability to indicate any actions of compromise and the relevant action of denying system access. In some cases, this action of denying system access can be automatic or can be manual based on the alert created for indications of compromise. One of the methods by which TPM takes this action is due to the unique key that is created by taking a baseline fingerprint of the server and its network functions as it boots. This baseline is then compared with measurements that are periodically taken from the system processes. If any change in the boot characteristic changes, then system access can be denied.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 279, 'parent\_id': '04b5c3406caf8c4158ac8417e0078559', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '38cf4b6fe2212ae3cb34e094db6fcac3', 'text': 'Although TPM solves part of the problem in MEC deployments, cloud-native deployment brings in a whole different angle to the topic of “trust” in 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 279, 'parent\_id': '04b5c3406caf8c4158ac8417e0078559', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2172348655ffc641f3cb55ac17b59299', 'text': 'This is one of the most important topics with my discussions with many customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 279, 'parent\_id': '04b5c3406caf8c4158ac8417e0078559', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '822f327c44d1c5d82752af107d096bab', 'text': 'The answer to this is to have multilayered security controls for the virtualized functions irrespective of where they are deployed. The applications (network functions and MEC applications) should have the flexibility to be deployed on premises, in the public cloud, or in hybrid mode (on premises and public cloud) and still be able to verify for trust. When data is transferred among networked systems, trust is a central concern. In particular, when communicating over an', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 279, 'parent\_id': '04b5c3406caf8c4158ac8417e0078559', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a194e5b814931f364b6df96582784ae9', 'text': 'untrusted medium such as the internet, it is critical to ensure the integrity and the publisher of all the data a system operates on. Some of the key security controls are discussed in the sections that follow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 280, 'parent\_id': '04b5c3406caf8c4158ac8417e0078559', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'db3cec572fa49edc52ec218a3a26a75f', 'text': 'Image Signing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 280, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bd6cd919618d3f84f3eb8c96f4b4a4bd', 'text': 'Image signing helps you validate the source of the software image and the authenticity of the image, thereby ensuring that the image has not been tampered with. You should ensure that the vendor you are choosing follows the image-signing process for both on-premises deployments and public cloud deployments, including VMs and containers. For on-premises deployments, some vendors require their dedicated hardware for their own specific software image verification, which might limit your deployment models, but it still ensures that you have a trusted image in your network. For container-based deployments (on premises and public cloud), the vendor should provide some sort of container registry mechanism where you can sign images to ensure their integrity in your registry namespace. This container registry should also provide an option for you to push and pull signed images. This will help you to validate whether the images are being pushed to the container registry by the Continuous Integration (CI) tools you own. One of the most used platforms in the container world today is Docker. In Docker, the Docker Engine is used to push and pull images to and from the public and private registry. Docker Content Trust (DCT) provides the ability to use digital signatures for data sent to and received from remote Docker registries. These signatures allow client- side or runtime verification of the integrity and publisher of specific image tags. Trust for an image tag is managed through the use of signing keys.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 280, 'parent\_id': 'db3cec572fa49edc52ec218a3a26a75f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fb659e4ca107f98201adbba96d264dc9', 'text': 'When DCT is enabled, only signed versions of the image can be pulled by you. For example, if you need an image of a 5G network function by Vendor A, Vendor A uploads a couple of image versions in the DCT. Once Vendor A signs the images, they can then be pulled. This ensures that you can pull only tested and signed images.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 280, 'parent\_id': 'db3cec572fa49edc52ec218a3a26a75f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd23a9485245ab4bd071beeca046b5668', 'text': 'Figure 5-31 shows a method of pulling signed images from the Docker Trusted Registry (DTR).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 280, 'parent\_id': 'db3cec572fa49edc52ec218a3a26a75f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'db6e8537769cee9a408e16d9281059d9', 'text': 'Load the signed Trusted Registry image in registry Signed Tag N Signed images only APIGW/ Vert.0 API FW 00— Sign Image —— | Production~ -~ I a Vert.0 > f Production M2M Vendor MEC Vendor E— Application Ver0.9 Test 5G Network function deployed in public cloud APIGW/ API FW Signed images only 0a 5G Network function deployed on-premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 281, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'fb9952f834773bdc50e39c2120075daa', 'text': 'Figure 5-31 Trusted Images Being Pulled from the Trusted Registry', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 281, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a4760cc27702e22cbefc9da5d0d5eee3', 'text': 'As shown in Figure 5-31, the vendor/developer signs the images and loads them into the registry. The registry contains both the signed and unsigned images. You can pull any 5G application-related images from the registry. When you request a pull for an image, only the latest signed image can be pulled from the registry. Once the signed image is pulled from the registry, it needs to be verified. This option is applicable to both the cloud and on- premises deployment models.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 281, 'parent\_id': 'fb9952f834773bdc50e39c2120075daa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e2e560acd4f9253d70192f0c579ae2ab', 'text': 'Secure Storage', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 281, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3dfc0f6fbe2e289234b361b70e9f4d85', 'text': 'While using the on-premises servers for MEC, you should ensure that the server provides highly secure storage for user credentials, private encryption keys, and other critical security information for the device. There are also very specific vendors providing a hardware security module (HSM), which is a physical device to protect and manage data at rest. The HSM you choose should be able to perform encryption and decryption functions for digital signatures, strong authentication, and other cryptographic functions. There are many varieties of HSMs; some are external devices that physically connect to devices such as PKI infrastructure, and some are plug-in cards typically used to back up the keys handled outside of the HSM.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 281, 'parent\_id': 'e2e560acd4f9253d70192f0c579ae2ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ded2878562c7791bffddc59547ea08ec', 'text': 'HSMs are usually designed to execute specially developed modules within the HSM’s secure enclosure, which is required in use cases where special algorithms or business logic has to be executed in a secured and controlled environment, such as for critical IoT 5G use cases in on-premises deployments of MEC. Due to the application of HSM in critical use cases, it is very important to ensure that you choose HSM vendors who have Level 4 testing and certification achievement in FIPS 140 (minimum FIPS 140-2). The use of a security gateway to protect MEC transport is explained in detail in the section “MEC Infrastructure and Transport Security.” Security gateways use PKI implementation for taking part in IPsec tunnel establishment and must have an RSA key pair and a certificate issued by a trusted Certificate Authority (CA). In PKI implementations, HSMs can be used by the CA to generate, store, and handle asymmetric key pairs. For 5G network functions, PKI-based certificate authentication can be used for TLS. If HSMs are used for 5G PKI-based use cases, they should support the following features to provide enhanced security:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 282, 'parent\_id': 'e2e560acd4f9253d70192f0c579ae2ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f071ef275e3b271612dd70f71977868f', 'text': '• Provide granular role-based access control (RBAC)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 282, 'parent\_id': 'e2e560acd4f9253d70192f0c579ae2ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6d7f3dcb4ecb8f5479781fe939cdf8ae', 'text': '• Secure key backup', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 282, 'parent\_id': 'e2e560acd4f9253d70192f0c579ae2ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '776ffd3d325290ead278428a428050a4', 'text': '• Support for multipart authorization schemas', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 282, 'parent\_id': 'e2e560acd4f9253d70192f0c579ae2ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd17388dc5ad5a940d93d71435da462d6', 'text': '• Blockchain readiness', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 282, 'parent\_id': 'e2e560acd4f9253d70192f0c579ae2ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4f62e91a207c4d338aee14d4d92a2fae', 'text': '• Support for multi-cloud integrations (at least the top three cloud providers in your region)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 282, 'parent\_id': 'e2e560acd4f9253d70192f0c579ae2ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f2c7ed69d1ef642637f294ceebce56b0', 'text': '• Implement quantum-safe algorithms', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 282, 'parent\_id': 'e2e560acd4f9253d70192f0c579ae2ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '487ed92aa49f45ef6d0173e185bb50ab', 'text': '• FIPS 140 Level 4 certified (minimum FIPS140-2, but FIPS 140-3 is even better)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 282, 'parent\_id': 'e2e560acd4f9253d70192f0c579ae2ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6c4ee30d7262efe0ebb5aae144edf0bb', 'text': 'Details on securing 5G CNFs in production, securing your network from the 5G NF and vulnerabilities, and compliancy of 5G CNFs are covered in the section “Securing Virtualized Deployments in 5G MEC” later in this chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 282, 'parent\_id': 'e2e560acd4f9253d70192f0c579ae2ab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f59a4d201c5c7b965dfff98c0a99e92b', 'text': 'MEC Infrastructure and Transport Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 282, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58842e81f3e428f06f71735b246f9445', 'text': 'One of the main reasons to use MEC deployment models is to enable URLLC use cases and allow the flexibility in deployment of 5G-related MEC applications as close to the edge of the network as possible. There are different models of MEC deployment, such as deploying the 5G network functions and MEC applications in the multistack public cloud, in the same location as the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 282, 'parent\_id': 'f59a4d201c5c7b965dfff98c0a99e92b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0409a546d23fca53ce8410c10b911f0e', 'text': 'gNB using servers with very low footprint, in far-edge data centers, in regional data centers, in hybrid cloud and on-premises models, and also enterprise data centers. As you have seen in the “MEC Infrastructure and Transport Vulnerabilities” section earlier in this chapter, the key vulnerabilities are due to MEC using the public network for the transport layer. This section will take you through the key security controls required to secure the 5G MEC deployments and methods to mitigate the MEC infrastructure-related threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 283, 'parent\_id': 'f59a4d201c5c7b965dfff98c0a99e92b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ccfe88cf9b6399ef009f24e1be6667c1', 'text': 'Figure 5-32 shows one of the methods to secure transport for on-premises deployment of 5G MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 283, 'parent\_id': 'f59a4d201c5c7b965dfff98c0a99e92b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '965d9e95fcee7342041c281a39657bec', 'text': 'Internet L Inspection of inbound and SP Services & Intemnet outbound Internet traffic AP communications between MEC and Internet over public network secured using TLS Application i aware NGFW [Secaw ) . 1 ) gNB . Centralized 5GC Transport over publi Transport over public network secured by network secured by |Psec using SecGW Attacker |Psec using SecGW', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 283, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd203235f2ee3ae2f3e96783004733225', 'text': 'Figure 5-32 Securing Transport for On-premises Deployment of 5G MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 283, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8456e1faa2b969fc46b5b9e64a0a61fb', 'text': 'The key security controls recommended for on-premises deployment of 5G MEC, as shown in Figure 5-32, are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 283, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'db3cb5a7490dc411597fe6bc06754f79', 'text': '1. IPsec between gNB and MEC: Security gateway (SecGW) can be used to provide an IPsec tunnel between the gNB and MEC if an untrusted public network is used as the transport between gNB and MEC. gNB requires mandatory support of the IPsec stack, which can establish IPsec tunnels natively; therefore, you don’t need a SecGW at the gNB location. You will require a SecGW at the MEC and centralized 5GC location.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 283, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'be0c554a558bce1405259321ab9aa7ab', 'text': '2. IPsec between MEC and Centralized 5GC: Depending on the location of the DU, CU, serving User Plane Function, and the control plane functions such as Access and Mobility Management Function (AMF) and Session Management Function (SMF) and the use of an untrusted public network, an IPsec tunnel will be required to secure the traffic traversing between the MEC and centralized 5GC. An example would be the traffic between the DU and CU, as shown in Figure 5-33.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 284, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '6ff65f96434ee48d9e042ec0c6970fb5', 'text': 'IPsec between Far edge IPsec between MEC & DC & Regional MEC Centralized DC 5GCP & Mgmt DU UPF- Far Edge DC Voice & loT Regional Edge DC Central DC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 284, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '53127f6a1afc0546372001b0943cad62', 'text': 'Figure 5-33 Example of SecGW Deployment Between DU, CU, and UPF', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 284, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '33829079c90ffbc20a441d94cfc231b0', 'text': 'Figure 5-33 shows the SecGW deployment between the DU and CU and between the CU and the centrally located UPF.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 284, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '59aaf3ee91de22810cc77dacfddf36e8', 'text': 'As shown in Figure 5-33, the traffic passing through the untrusted public network is protected by the SecGW:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 284, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4a9c8195b84d375d05a53942d239672c', 'text': '1. API GW/API FW between MEC and Centralized 5GC: To secure API communications such as between the 5G CNF components and orchestration, an API gateway (API GW) or API firewall (API FW) is recommended between the MEC and centralized 5GC. API security has been explained in detail in the “Securing API” section of this chapter', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 284, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c1416de4d36adb181d8efb5bad4da65c', 'text': '2. API GW/API FW between centralized 5GC and services deployed in the Internet: To secure the API communications between the centralized 5G network functions and services deployed in the Internet, an API gateway (API GW) or API firewall (API FW) is recommended between the MEC and', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 284, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd6c6ac99ee9e92a707f4d5e389036815', 'text': 'centralized 5GC. An example could be data analytics layer API security, which has been explained in detail in the “Securing API” section of this chapter', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 285, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7ed57939f0ef32a912488e9d844cab3d', 'text': '3. NGFW at the MEC location: To inspect the traffic from the MEC applications and 5G CNF, such as UPF, a next-generation application-aware firewall (NGFW) is recommended. This firewall is aimed at ensuring that 5G CNFs are using only authorized ports and protocols and also inspects the incoming packets for any abnormalities. This NGFW should also be able to provide URL filtering and have integrations with threat intel for creating automatic rules based on indicators of compromise (IoCs).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 285, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '99237297055afd35283f9165656e82f7', 'text': 'Figure 5-34 shows one of the methods to secure transport for hybrid deployment of 5G MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 285, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a54706e9862e3b87886b06c8d3692a6e', 'text': 'Public cloud deployed 5G core services & Internet Public cloud deployed MEC services Attacker MEC CU, UPF 5GC CP (AMF, SMF, PCF ....) e g e Applications S o] SecGW required only at /,-/Ik( AA’::!IGF‘\\IIVV/ : Ay E - e - - CU location to aggregate IPsec from multiple DU X AP| communications Transport over public over public network network secured by IPsec > secured using TLS x - - - s I f (Lapi P ) SecGW R e e NMS, EMS, Billing, ((A)) Senvice Provider if@f" i i( i Orchestration Front Haul / Mid Haul gNB MEC Centralized 5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 285, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f194afed006bbcb6f6e3287b7a380a40', 'text': 'Figure 5-34 Securing Transport for Hybrid Deployment of 5G MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 285, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '68666213c2df397ba342455b7d0a40eb', 'text': 'The key security controls recommended for hybrid 5G MEC deployment, as shown in Figure 5-34, are listed here:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 285, 'parent\_id': 'f194afed006bbcb6f6e3287b7a380a40', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f9076158120122665fe6059e11736d92', 'text': '1. IPsec between MEC and public cloud: In this deployment, the DU is deployed in the far edge DC, while CU is deployed in the public cloud. The public cloud virtual instances also include MEC applications and the user plane functions. IPsec implemented by SecGW is recommended to secure the traffic in the F1 interface, which is between the CU and the DU. F1-C is the interface between DU-CP and CU-CP, and FI-U is the interface between DU-UP and CU-UP. Only the CU locations need the SecGW implementation, as the DU supports an embedded IPsec stack to support initiation and termination of IPsec tunnels between the DU and SecGW at the CU location.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 286, 'parent\_id': 'f194afed006bbcb6f6e3287b7a380a40', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bed3f001543b719328fe9661ed89ebb7', 'text': '2. API GW/API FW between MEC and public cloud: To secure the API communications using an untrusted public network between any MEC clients deployed on the MEC and the MEC application server deployed in the public cloud, it is recommended to implement an API GW/API FW. The API FW is also sometimes called Web Application Firewalls (WAF) by firewall vendors.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 286, 'parent\_id': 'f194afed006bbcb6f6e3287b7a380a40', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6db45c2d4ada1e6885ad7abe65820d70', 'text': '3. API GW/API FW between MEC and centralized 5GC: To secure the API communications using an untrusted public network between any MEC and centralized 5GC, such as API calls from the orchestration layer, it is recommended to implement an API GW/API FW.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 286, 'parent\_id': 'f194afed006bbcb6f6e3287b7a380a40', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ca101a7c6a75c0e0746e1f1254c5aad7', 'text': '4. API GW/API FW between centralized 5GC and public cloud: To secure the API communications using an untrusted public network between centralized 5GC and the public cloud, such as API calls between the billing and 5GC charging functions, it is recommended to implement an API GW/API FW.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 286, 'parent\_id': 'f194afed006bbcb6f6e3287b7a380a40', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '88b2ac23e2b121e22b732157a216f4d3', 'text': '5. IPsec between centralized 5GC and public cloud: In this deployment, the 5GC control plane functions are deployed in the public cloud. The IPsec implementation is recommended to secure non-API communication between 5GC centralized network functions and 5G control plane functions deployed in the public cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 286, 'parent\_id': 'f194afed006bbcb6f6e3287b7a380a40', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7b1272f9dc01adf2068ba181b84ee40e', 'text': 'Figure 5-35 shows one of the methods to secure transport for RAN location– deployed 5G MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 286, 'parent\_id': 'f194afed006bbcb6f6e3287b7a380a40', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '35f2e7abb2cdf12abaf610acda4420e6', 'text': 'SecGW deployed at CU location to terminate IPsec tunnels from multiple DUs CU, UPF [ 4 - MEC application APIGW / [ API FW MEC - Public cloud & Internet \* On-premise based virtual DUs x X L Security policies for user, connected to CU deployed in device and API enforced MEC hosted in public cloud » by the API GW / AP FW using F1 interface - IPsec tunnel established using o° embedded IPsec stack in DU AP| communication software <(A)) secured by TLS and the AP| GW / AP| FW security policy enforced by \\ RAN site hosted DU & MEC client in least-footprint server', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 287, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '05a051e9446414243079ea6b0635e8f7', 'text': 'Figure 5-35 Securing Transport for 5G MEC Deployed in Low-Footprint RAN Node Server', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 287, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5238ca0465cc460e1f3e42e1c9f819c0', 'text': 'The key security controls recommended for 5G MEC deployed in a RAN location, as shown in Figure 5-35, are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 287, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '448526b2b1416201b7840d6366f07bca', 'text': '1. IPsec between DU in MEC and CU in the public cloud: In the example shown in Figure 5-35, the DU control plane and user plane are deployed in the RAN location within a low-footprint server, and the CU control plane and user plane are deployed in the public cloud along with the UPF. Another variant could be DU–UP, DU-CP, and CU-UP deployed in the RAN node location and the CU-CP deployed in the public cloud. But as the CU allows aggregation of multiple DUs, and if you want to have the server as low footprint as possible, it’s best to have the CU-CP and CU-UP deployed in the public cloud. In this case, the F1 is protected by the IPsec tunnel, which is supported by the DU software stack, which is terminated by the SecGW deployed in the public cloud, which is aggregated toward the CU-CP and CU-UP.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 287, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9a0d1a3c169aaa2312e081935ca25313', 'text': '2. API GW/API FW between MEC and the public cloud: To secure the API communications using untrusted public network between any MEC clients deployed on the 5G MEC deployed on the RAN location and the MEC application server deployed in the public cloud, it is recommended to implement an API GW/API FW. The API can be protected by using TLS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 288, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ef99c3af10132f8966a0da728a79f138', 'text': 'Figure 5-36 shows one of the methods to secure 5G MEC deployed in enterprise data centers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 288, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '1c5c00e16a90ab6105fe17b86164dbad', 'text': 'Attacker \\ [ — OAM IPsec using SecGW secures N2, N4 & N9 traversing over APIGW/ 5G CP functions public network AP| E MEC Application T Bl () Centralized 5GC AP| communication secured by TLS N2 and security policy enforced by the N4 APIGW/APIFW N9 p P [ e T ey ko \_S\_ecGW APIGW/API FW jl ‘= M2M devices DU, CU, UPF Q M2M Vendor M2M MEC Application MEC Application K e - Enterprise DC Enterprise MEC deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 288, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '336e16326c18ebbc54c808f34896a3db', 'text': 'Enterprise MEC deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 288, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b3a23976bafa9b8e64af0c40e641f126', 'text': 'Figure 5-36 Secure Transport for 5G MEC Deployed in Enterprise Data Centers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 288, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '945d7445944a27a9ade8735c8a1e2d81', 'text': 'The key security controls recommended for enterprise network–based 5G MEC deployment as shown in Figure 5-36, are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 288, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '00893939f111f78fbc462253a1cf2070', 'text': '1. IPsec between enterprise MEC and centralized 5GC: The DU control plane and user plane, along with the CU control plane and user plane, are deployed in the enterprise location. The following interfaces would traverse the untrusted public network:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 288, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1b97e2473116ffbc1e0f12413ac3638a', 'text': '• N2: Interface between gNB-CU-CP and AMF or gNB and AMF (depending on deployment)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 289, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f93f18615b5a0db343a153a1bcdd6f48', 'text': '• N4: Interface between UPF and AMF', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 289, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fc91edfe7fa8a74b896cf6231f2f5375', 'text': '• N9: Interface between UPFs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 289, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7db1ad50ca58aab0f5533acbfb9f0e74', 'text': 'To protect these interfaces from any eavesdropping or MitM attacks, it is recommended to use IPsec catered by SecGW between the enterprise MEC and 5GC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 289, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4062f0999a4b2b4a0c486e21a726213c', 'text': '2. API GW/API FW between enterprise MEC and centralized 5GC: To secure the API communications using an untrusted public network between any MEC clients deployed on the 5G MEC deployed on the enterprise location and the MEC application server deployed in the centralized 5GC, it is recommended to implement an API GW/API FW. The API can be encrypted using TLS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 289, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b880665c8ae633fa24318059db85b238', 'text': '3. API GW/API FW between enterprise MEC and the public cloud: To secure the API communications using an untrusted public network between any MEC clients deployed on the 5G MEC deployed on the enterprise location and the MEC application registry hosted by the MEC application vendor, it is recommended to implement an API GW/API FW. The API can be encrypted using TLS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 289, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8523bba79dacddc62f6af5815759adbd', 'text': 'Apart from the SecGW and API GW/FW use cases mentioned in this section, it is also important to provide segmentation and isolation between the enterprise MEC and the centralized 5GC. This can be provided by configuring zones within the data center network and then implementing granular access control policies. You must write specific security policy rules to allow traffic to pass between zones, so only traffic that you explicitly allow can move from one zone to another. The isolation can be further enhanced by using Security Group Tags (SGTs) functionality provided by vendors in the market and then apply policies based on those SGTs. SGTs provide unique security group numbers that are assigned to the security groups, thereby allowing for segmentation without needing VLANs. The security groups are the list of users and endpoints that require similar access control. Having this flexibility will enable you to deploy granular isolation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 289, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '46cc9c9b13e2a4f8171beb49cef2e8b7', 'text': 'Malware detection and response is another key security control required in MEC deployments. For 5G deployments, you will require next-generation malware implementation. The chosen anti-malware solution should build a full real-time context around every process executed and use machine learning', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 289, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b75b6b5969361e92aab1de8c6ff0e34f', 'text': 'models, which identify patterns known as malware characteristics and various other forms of artificial intelligence.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3ea08755dc00ad3af14a116b7e250b10', 'text': 'Securing Virtualized Deployments in 5G MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a129a3567a41e52397c06dd62b4c2fa9', 'text': '5G standalone (SA) deployments are primarily cloud-native network functions (CNFs). This means that the containerized functions should be able to be deployed in any infrastructure and public cloud provider without impacting the interoperability and specific functions. While it sounds really flexible and scalable, care has to be taken while deploying such functions. Apart from the embedded security controls discussed in the section “Hardening Hardware and Software” in this chapter, there needs to be multiple layers of security to ensure that the cloud-native deployments of 5G network functions and MEC applications are protected. We should also ensure that these virtual functions are also secured, and any data exfiltration is detected and stopped.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b4312d4fb6c708b7a40655ae59fdf369', 'text': 'Securing the cloud native functions and containers is discussed in detail in Chapter 6, “Securing Virtualized 5G Core Deployments.” This section is aimed at securing virtualized deployments specific to 5G MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a1209a50e3d6866dd26c00b39d827489', 'text': 'The location of these functions within the network are also important before deciding the security controls. Some of the locations, such as low-footprint servers, are very lightweight deployments that sometimes have no separate rack or shelter to accommodate the security appliances. The different locations for MEC deployments are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2e3f85720c72ef6dfe5d92cbb3135c4b', 'text': '• RAN node location', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8751b6402ec7adb95fb7979433694b90', 'text': '• On premises (far-edge, edge, regional data center)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a6b93b37a68238ceacc7f5c145773d8f', 'text': '• Cloud-based deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '94775c2fb1b23dd45a86f6cb785e6436', 'text': '• Hybrid deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9bd2aefc5378e9571ddcc00ff811d1aa', 'text': '• Enterprise location', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1adc2ab31816b0e7f640dc713d8784c4', 'text': 'The virtualized 5G-related network functions expected to be deployed in MEC are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6fafeea01ccceea339f7da451a730ee9', 'text': '• Virtualized DU', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '893c667acac2b8819851210fc5ad5d42', 'text': '• Virtualized CU', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd71f98b241bef52a3b8ad69076f397d2', 'text': '• Virtualized user plane functions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 290, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a986246aaa3e41f674bb97617da57e99', 'text': '• Virtualized control plane functions (some functions only, in specific circumstances)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 291, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c71261516a4e0760a4dd6d3ad10ebaf2', 'text': '• Subscriber authentication and policy functions (IoT related, apart from the 5G control functions)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 291, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a88ec74c9d563fa43e065ae055ef9926', 'text': '• IoT applications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 291, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a1b74d77a868aebfb64d7bdb674d75e', 'text': '• M2M applications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 291, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dd46b8c5d93020e60ad78f8f01f62125', 'text': '• Enterprise applications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 291, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e786c9418bd9364e05c36a8d499e68b2', 'text': '• MEC applications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 291, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b73d10d5182978dd555d2136d86e4861', 'text': 'All the virtualized network functions described in the list will be mainly cloud- native containerized functions deployed on virtual machines, bare metal, or in the public cloud. In this section, we will discuss the different security controls to secure the virtualized network functions and security controls to secure the MEC infrastructure from vulnerability in the virtual functions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 291, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d5f2484762a854200adf50289e3ee52', 'text': 'Figure 5-37 shows the recommended security controls to secure the virtualized network functions and applications in MEC deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 291, 'parent\_id': '3ea08755dc00ad3af14a116b7e250b10', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd9ed55d29cec66936f86a82e8e4680b6', 'text': 'Nodation s 5G Network function deployed in public cloud Provide visibility on all deployed virtual / cloud native network functions Vulnerability assessment for all virtual components Container Runtime security Provide security to the orchestration system (both VM and containers) g Secure all external interfaces a Secure all internal interfaces Provide visibility on all users accessing the network components User User access controls based on zero trust principles Provide Forensics capabilities and process behaviour detection > Bed Micro-segmentation Anomaly detection (data leakage, exploit detection) Compliancy and Audit capabilities = = " = = = = o= omo=o=om o= == 0 Protection against lateral movement of malware 5G Network function deployed on-premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 291, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a8e9f619766aee14dd1e81be71a96af4', 'text': 'Figure 5-37 Recommended Security Controls to Secure the Virtualized Network Functions in MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 291, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ca5418f1f35f9e6478180b94c619f473', 'text': 'As shown in Figure 5-37, true security for the virtualized deployments in MEC also needs to consider non-virtual components as well. This includes internal and external interfaces of the on-premises server where the virtualized components are deployed on MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 292, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d6a35d479ecbc90f60b2a8589434fba', 'text': 'Figure 5-38 shows an example and method for image scanning, analytics, and the application policy enforcement layer for securing the virtualized deployments in 5G MEC. The recommended practice is to use the private repository for your 5G RAN and core CNFs and use the public repository only for the 5G MEC applications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 292, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c04493dabb6f053f81219f6d9b96f564', 'text': "Threat Intelligence Rl SR R SN R s, S e Pull images MEC hosted in Public cloud \\ OConlamer Telemety, User defined rules L VM Telemetry, ol Network Telemetry, —| ‘l 4 User Identity in Wit - - - - - - Cl/CD - - - Image Scanning, Analytics and Application polcy enforcement Engine ). Aol i d [ lui | . . i = (T VM Vulnerability & exposure tracking RAN-Site low - . fr——— ( = Image vulnerabilty tracking S SR S S = Alerts based on detected anomaly footprint MEC On-premises MEC é Policy simulation Automated ' Integration with SIEM layer R Microsegmentation policy \* Detect malicious behaviour based on application \* Detect crypto jacking behaviour = / \\ Ebaay e sl e o Enterprise deployed MEC l.‘\_", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 292, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a50db246406114e0c0e9fe3c679097c5', 'text': 'Figure 5-38 Multilayered Security Control for Securing Virtualized Deployments in 5G MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 292, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '080465ad3951200b533b1d25b667ce58', 'text': 'As shown in Figure 5-38, securing virtualized deployments would require multilayered security controls. The security controls should be able to be enforced irrespective of the location (public cloud, on-premises MEC, enterprise data center) the virtualized network function/MEC application is deployed. The security policies should be consistent wherever the 5G network functions and MEC applications are deployed, be it bare-metal servers, virtual machines, or dynamic environments like containers and microservices in on- premises or public cloud. The security controls and capabilities shown in the Figure 5-38 are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 293, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4078f3babda0bf1472477dc17379a431', 'text': '1. Telemetry collection: The solution should have a robust telemetry collection to create an accurate baseline of the network. The telemetry collection should include telemetry such as NetFlow, Internet Protocol Flow Information Export (IPFIX), sFlow, and other types of flow data from your multivendor MEC infrastructure such as routers, switches, firewalls, endpoints, and other network infrastructure devices. It should also receive and collect telemetry from proxy data sources, which can be analyzed by the cloud-based, multilayered machine learning engine for deep visibility into both web and network traffic; this includes container sidecar components, inter- and intra-microservices communication, and it should be able to consume logs from the public cloud. The security controls should provide visibility on all deployed virtual components. The virtual components include virtual components such as VMs, CNF as containers deployed on a VM, bare metal, public cloud, and hybrid cloud environments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 293, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'db77a6a248a79910cc192d17fd3d2ee2', 'text': '2. Image scanning and vulnerability assessment: The security controls should provide the vulnerability scanning for test and production MEC environments. Any images of 5G CNF and MEC applications should be verified and checked for any vulnerability before being deployed on your production pods. Once deployed, the vulnerability assessment should include vulnerability tracking against known Common Vulnerabilities and Exposures (CVEs). The vulnerability scanning should include all forms of virtual components (VMs, CNFs, containers on VMs/BMs/public cloud). The security controls should provide a secure build, deploy, and run process; this includes any DevOps process, which includes the process of signing and tagging any images built by you and loaded in the container registry, GitHub, or serverless deployments for MEC applications. The platform providing the security control should include compliancy controls and runtime policy. User-defined policies should be able to be enforced on the trusted and verified images. Validation of compliancy should include', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 293, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c54e46414dfa0afa1b01dda4522202c1', 'text': 'benchmarks from PCI-DSS, NIST800-190, NIST800-53, CIS, and so on, which should be automated. The audits should also be carried out for the orchestration component used for your deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 294, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'abe370007db69f7691a9f03253e82429', 'text': '3. Threat intelligence: The platform providing the security control should have a global threat intelligence feed to stop any threats that are seen in any other part of the world. The platform should also maintain an up-to-date CVE data feed from multiple sources, including NIST and OS vendor data packs, which contain the latest vulnerability and exposure information.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 294, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b1c3ce49b59a44c3fc020b0e4a27b1b2', 'text': '4. User-defined policies: You should be able to configure user-defined policies for specific 5G CNFs being deployed on the MEC. Once the image is verified and trusted, specific policies should be able to be enforced on the image. The security controls should provide granular access control and include or be able to integrate with controls such as multifactor authentication (MFA) and role-based access control (RBAC). The user-to- application mapping should be part of the baseline, and any anomaly should be identified and alerts/events created for it.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 294, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '428f582edae2a0d54fc5bfb7860a6d8e', 'text': '5. CI/CD integration: The CI/CD workflow integration is crucial for robust security control, specifically if you have a DevOps team uploading images for MEC applications that might be developed in house by your team. Any images being uploaded by your development team in a registry, GitHub, and so on should go through the vulnerability scanning process to detect any vulnerabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 294, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '275d9dd39f7bc345f5cb6658a7334e80', 'text': '6. Micro-segmentation and anomaly detection: The security controls should enable automatic micro-segmentation based on the initial baseline considered for deployment. The micro-segmentation process should also consider 5G CNF-to-services mapping. An example of services is DNS requirements. The micro-segmentation layer should be able to enforce the micro-segmentation policy across all virtual components and deployment locations (on-premises/public cloud/hybrid). The security controls should provide anomaly detection based on behavioral analysis on the initial baseline. The baseline should also include a process baseline and be able to identify deviations for faster detection of indicators of compromise (IoCs). The anomaly detection engine should be integrated or have built-in machine learning, behavior analysis, and algorithmic approaches to ensure that lateral movement can be identified and contained.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 294, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'bce5841c7ba23f67afd13ed2555d6008', 'text': 'Build, Deploy, Run', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 294, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1e3f0debfeb1efbe4fa560138c10f240', 'text': 'It can be overwhelming to track all vulnerabilities. The solution is to have a good process to determine which vulnerabilities are relevant to your organization. This prevents overreaction and the mistakes that can be inherent to rapid, poorly planned upgrades or configuration changes.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 295, 'parent\_id': 'bce5841c7ba23f67afd13ed2555d6008', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9cee4b79ee967cafa37aea76694abe07', 'text': 'Figure 5-39 shows the secure runtime environment with secure build, deploy, and run processes, further described in the list that follows.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 295, 'parent\_id': 'bce5841c7ba23f67afd13ed2555d6008', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '95dfd0f2b6c8aee7e75bf87162dfbe1f', 'text': '3 User Defined policy 4 5 6 — : Continuous ‘ Image from ;Image Scanning Enforce user trusted & Verification defined policy repository ———— Deploy ‘ ——— Build ‘— Run —‘', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 295, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd2c87749d666e8d31996cc891c3f5805', 'text': 'Figure 5-39 Secure Runtime Environment with Secure Build, Deploy, and Run Processes', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 295, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9886efa261a57e7ee6c8c9271dd1e204', 'text': 'Step 1. As described in the section “Hardening Hardware and Software” within this chapter, only trusted registries should be used for loading the signed images by the vendor. You should push/pull only signed images from the trusted registries.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 295, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b5d7b940fef89b1202a3a553af4ce134', 'text': 'Step 2. The push and pull images should undergo scanning as part of the CI/CD pipelines and runtime deployments to detect vulnerable images. If any vulnerable images are found, then the security control should prevent the creation of a pod.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 295, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '92a6245a100685af72826c294f4bc2f1', 'text': 'Step 3. For 5G MEC deployments, it is important that you can define and enforce policies for the 5G network functions and MEC applications, such as for user plane functions (UPFs), Centralized Unit (CU) and Distributed Unit (DU), and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 295, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bcb15c0adca7c0f0acaf6a6adca02bcc', 'text': 'Step 4. The verified and trusted images can now have user-defined policies being enforced so that you can deploy images with the right polices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 295, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '304029daae2f5ce8f9cb3353bdc1a2b5', 'text': 'Step 5. Once the images are verified and trusted and specific policies are enforced for the images, the next step should have the automated configuration check before it is deployed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 296, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '269d05baed829fdac0ea940c8d2c12c3', 'text': 'Step 6. The deployed images should be under continuous monitoring and be tracked for any vulnerability against the databases of known CVEs. Having anomaly detection engines would help you detect any lateral movement between the MEC virtual components.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 296, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5fbf9136d0933686b19c17fab7aef76e', 'text': 'Side-channel attacks occur due to vulnerabilities or due to methods of exploiting the measurements of the chipsets (mostly crypto chipsets), which leads to leaking of information. There are many variations of side-channel attacks, such based on time attacks, which are based on the fact that different operations or input values have a significant time variance. Using this information, the attacker can deduce the secret key from the cryptosystem. Another attack vector is based on the attacker performing waveform and amplitude of voltage peaks used by the system, including the idle values and active (during operation) values, which are then compared with the known values for certain operating system software.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 296, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '26989b32f9ee51f8816694f6477ca237', 'text': 'These attacks can be passive or active attacks. A passive attack is when the attack simply involves listening to the environment emissions caused by the circuit. In a passive attack scenario, the attacker uses passive monitoring devices such as a receiver antenna in close vicinity of the equipment to monitor the clock frequency of the CPU used in the circuit and capture signal waveforms to retrieve secret information. An active attack is when the attack involves tampering with the operations of the circuit. In an active attack scenario, methods such as power tracing based on the measurement of the current drawn by the chipset from the supply voltage is traced and then compared to the database consisting of known current consumption values of targeted software and hardware circuits and chipsets. In such attacks, the attacker would require a power-tracing chip or circuit between the targeted chipset and the power supply.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 296, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '24609a11c7c05910f8065be2b7639ee1', 'text': 'There are multiple ways of mitigating these attacks. Mitigation of some of these attack vectors will require software and firmware updates and patches, a secure supply chain, and a very secure physical facility to cater for many of the known vulnerabilities. But the key threats are from the unknown vulnerabilities or vulnerabilities that are not yet exposed. Quantum computing brings in a whole different perspective and requirement of threat and risk analysis required', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 296, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0ee7a9104127426136c1dba8ee58abd5', 'text': 'to be done to the entire MEC infrastructure, but that is better covered in Chapter 12 “5G and Beyond.”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 297, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '78fad3404b313a426261cb9fcdde1789', 'text': 'Figure 5-40 shows an example of one of the methods for mitigating side- channel attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 297, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '66eaa168d5c74922c88578a93ef24350', 'text': 'Telemetry from Multi Vendor components (Network devices, vSwitches, VMs, Containers, — syslogs etc) (2) Baseline network and ol . application pgh\_a\_viour u\_sing > enhanced visibility engine MEC application > = = S 2 A A 9 e I —— . = ®|® Wiy <-----—-- S N = ® [ I i Policy C2C server Storage server enforcement to e » ‘.. E resolve detected Block C2C server anomaly connections \\ MEC server { S Mitigation of MEC Data exfiltration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 297, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b0c1a9e58b52b25ca85953bd83bbb24e', 'text': 'Figure 5-40 Example of Side-Channel Attack Mitigation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 297, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c177cee34a4f42b278e7da1592d9c632', 'text': 'Figure 5-40 shows one of the countermeasures for side-channel attacks. The key preventive method for side-channel attacks is to use chipsets that are resistant to or have built-in capabilities against known side-channel and fault injection attacks. But the fact is that the chipsets are never fully resistant against side-channel attacks. It is important that the service providers and enterprises build a security mechanism to detect data exfiltration and contain the threat by not allowing it to get out to the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 297, 'parent\_id': 'b0c1a9e58b52b25ca85953bd83bbb24e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '338a59a3043abade90c6b2750ff798e7', 'text': 'Let’s look at the steps in one of the methods for mitigating side-channel attacks by using the detection and mitigation system illustrated in Figure 5-40.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 297, 'parent\_id': 'b0c1a9e58b52b25ca85953bd83bbb24e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd2638b7d673bfe101602ddf0e39088e6', 'text': 'Step 1. Network and user metadata is collected from various sources (network devices, virtual machines, container hosts, containers) and fed into the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 297, 'parent\_id': 'b0c1a9e58b52b25ca85953bd83bbb24e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '00233c28829644a5a5bb0247a9339671', 'text': 'enhanced visibility solution.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 298, 'parent\_id': 'b0c1a9e58b52b25ca85953bd83bbb24e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4c92cfcbbe77817719725fb4f0eab423', 'text': 'Step 2. As shown in Figure 5-41, for the enhanced visibility layer to identity any anomaly in the network, there needs to be relevant data to be fed into the system.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 298, 'parent\_id': 'b0c1a9e58b52b25ca85953bd83bbb24e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'b1f0a50f22dc879c485e22db07e0bb4f', 'text': 'Threat intelligence l Multivendor NetFlow (NetFlow / Sflow / IPFIX etc. Hypervisor metadata Baseline network and application Detect anomalies On-premises Container Telemetry behaviour using enhanced in traffic Cloud Container Telemetry visibility engine User |dentity Machine Learning & Artificial Intelligence algorithms', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 298, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '717818e555a3d4443b54e8986caaa117', 'text': 'Figure 5-41 Enhanced Visibility Layer to Identity Any Anomaly in the Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 298, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f40ae67cad582ebbf806ea6f0031804c', 'text': 'An enhanced visibility solution needs to be able to use a combination of different methods. It begins by collecting data from multiple layers and combining them for comprehensive visibility. Once data is collected from the right sources, a baseline of normal behavior for network devices, applications, and users could then be created. The next step is to apply machine learning. The solution then needs a robust threat intelligence input that is aware of malicious campaigns and maps the suspicious behavior to an identified threat for increased fidelity of detection. This should be the bare minimum required to thwart attacks that might have crossed the perimeter, or even threats originating within or are hiding in encrypted traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 298, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9773a1bcb6ebe224792df5eea6b3f67e', 'text': '• Network telemetry: This is composed of data sources that can provide useful insights about who is connecting to the network and what they are up to. It includes a multivendor collection of packet flow, syslog, SNMP information from network device exporters, switches, virtual switches, and includes formats such as NetFlow,', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 298, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '123c7606cfd9ebbc6464a4f43da11d6f', 'text': 'jFlow, sFlow, IPFIX, Netstream, SNMP, NSEL (NetFlow Secure Event Logging), and syslog.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 299, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a4c9c5090429f30382b77d927ac55539', 'text': '• Hypervisor metadata: Hypervisor metadata is the metadata collected from various hypervisors deployed in the infrastructure. The most common sources of hypervisor metadata is from hypervisors such as ESXi and KVM.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 299, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dd4454d062ef067bf64a09b802b69c96', 'text': '• On-premises container telemetry: On-premises container telemetry includes the container’s telemetry deployed on the premises of the service provider or enterprise MEC. One of the sources for container telemetry is Kube-state-metrics, which is a simple service that listens to the Kubernetes API server and generates metrics about the state of the objects, such as deployments, nodes, and pods. The other common sources are Kube-state-metrics for Kubernetes hosts running on Kubelet is from the node exporters like Prometheus, which would expose telemetry data for system resources on an HTTP endpoint.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 299, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c2f9350e361e52f287289422e78ef13b', 'text': '• Cloud container telemetry: Cloud container telemetry is the container telemetry for MEC applications deployed on the public cloud. Public cloud providers normally provide out-of-the-box monitoring for the containers deployed in their cloud infrastructure. In many instances the service providers and enterprises going for the cloud deployment of the MEC functions require the logs to be collected and visualized on an on-prem solution to have end-to-end visibility. In such circumstances, the chosen vendor should be able to collect flow logs from the cloud provider and perform various types of flow analysis.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 299, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '99f71a5ef1a961e1bdc5852d48d7eec9', 'text': '• User identity: User identity information is the information gathered by an existing IAM (Identity and Access Management) solution. This information will further enhance the intelligence gathered from the network device, virtual machines, and containers. The mapping of the users/user devices and the network and application flow information would help the host quarantine mechanisms in case of any hosts get infected.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 299, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a4c9b0b9cd51c4ae797a607fd889a92b', 'text': '• Threat intelligence: Threat intelligence is the global information about threats and threat actors, which can be fed into the enhanced visibility engine to act against known threats and threat surfaces. The threat intelligence is usually collected from multiple sources,', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 299, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f6d282d43760c36cd0fd1c0fc3b507e9', 'text': 'including the deep and dark webs. The main intention is to detect threats that are previously known and make informed decisions about them.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 300, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0233a5d1cc72614462ace832d0bba7c3', 'text': '• Machine learning and AI algorithms: This is one of the most important parts of the enhanced visibility engine. The attack vector, which would be quite unique to 5G due to its deployment methods (open-source cloud-native functions), is zero-day attacks. These are attacks that have never been seen before, hence the name “zero day,” and are typically due to vulnerabilities in the virtual and open source components used for 5G network functions. Machine learning and AI algorithms could apply predictive analysis and various mathematical models to the collected data and threat intel for any prediction of attacks. A fine-tuned model, along with the collected network and user information, will help determine any attacks beforehand.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 300, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '70fc10a00046c93ec1014891de7b11de', 'text': 'Step 3. Once the analysis of the data is completed and any anomaly is detected, the solution can take an appropriate action. In this example, the enhanced visibility solution finds a thin stream of data being continuously exported out of the network. The enhanced visibility solution also understands from the analysis and threat intel that the server is a part of a malicious network. The enhanced visibility engine (EVE) now comes to the conclusion that the data being sent out is part of the data exfiltration procedure being carried out by malicious actor.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 300, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0b01faf880c860c909c65c92ca64c09d', 'text': 'Step 4. EVE then sends out the command to the network device (switch/router/vSwitch) to terminate the connection to the external server and suspend any communication with it.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 300, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd073a401ee085e4ba21a156a52dad7f6', 'text': 'Step 5. EVE also detects that the inbound traffic from the malicious server (if any) can be blocked or directed to a sinkhole/quarantine-segmented network to prevent alerting the malicious actor.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 300, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dcc82c4190a65ffe0c3df448f558c3d6', 'text': 'As explained in this example, the data exfiltration can be detected using an enhanced visibility engine with the help of data collection from the right sources, robust threat intelligence, and a well-trained machine learning and artificial intelligence algorithm.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 300, 'parent\_id': '717818e555a3d4443b54e8986caaa117', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c31d1eb2f5842abb97b921b5d6feb5fb', 'text': 'Securing API', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 300, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '59e42a9b94afbf26816d2973508398e9', 'text': 'API security is a very critical security control for securing the MEC and the 5GC cloud-native functions. Although TLS is used for protecting the API and is recommended as part of securing service-based architecture (SBA), there are threat surfaces where malware or DDoS attacks could be orchestrated using the encrypted layer as well. Let’s look at the enhancements that 3GPP is working on as well as other mechanisms to secure the API.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 301, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2ac6cb7fe4bfefc6899ebec5b024a52', 'text': '3GPP is working on a framework for the unified northbound API framework across several 3GPP functions, called Common API Framework (CAPIF), to help secure the APIs and have a common service platform for 5G implementations and use cases, many of which would be deployed on the MEC layer. Another activity specific for 3GPP edge deployments is the application architecture for edge apps (EDGEAPP).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 301, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4cc292f0499b570afbbe870ef9fd553d', 'text': 'CAPIF was delivered in Release 15, with enhancements coming in Release 16, and is integrated with the northbound APIs developed by 3GPP SA2 (SCEF/NEF) and 3GPP SA4. The CAPIF architecture is specified in 3GPP specification TS23.222, “Common API Framework for 3GPP Northbound APIs,” and Figure 5-42 illustrates the functional model (version 16.8.0, Release 16).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 301, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '4bee09be5630ab5ea3406a2f6db0da76', 'text': 'APl invoker I [T LT T MO Tt N N AR e e L R e L M e P S T ST P P CAPIF-1e APl invoker J CAPIF-2 CAPIF-7 CAPIF-2e PLMN CAPIF-1 Trust Domain & Comense S el - rvice APls | CAPIF-3 AP exposing function CAPIF-4 CAPIF APIs AP publishing function (CAPIF Core Function) CAPIF-5 ! API management function API provider domain At SINE SelSeniat SeSCdant Satceess heLionEl heochiE Sl oG Soleas miaeeni o SEok e NamE e e eeie', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 302, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1bb58f65327644f75abefcd057aaded5', 'text': 'Figure 5-42 Functional Model for CAPIF (Source: 3GPP TS23.222)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 302, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd5c5e6619bee25204a43323426bd47e4', 'text': 'Figure 5-42 shows the functional model for the common API framework (CAPIF), which is organized into functional entities to describe a functional architecture that enables an API invoker to access and invoke service APIs. The key functional entities are CAPIF Core Function (CCF), API Exposing Function (AEF), and the API Invoker. The CCF is the central repository for all of the APIs, taking care of authentication, on-boarding, and aspects related to logging and charging. Key details specified for these functions in TS23.222 are listed next:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 302, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a0aab54700a0265293567bb00ea993e7', 'text': '• CAPIF Core Function (CCF):', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 302, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e9479393f540e8adaf9622ec0cc22e65', 'text': '• Allows discovery of stored APIs by the API Invoker using CAPIF-1 (PLMN trust model), CAPIF, 1e (outside PLMN trust model), and with API-exposing functions using CAPIF-3', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 302, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '06cdd1ada67a5dc0225a75b94b05a76d', 'text': '• Provides authentication and authorization for API invokers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 302, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '16128b361001cfbb86f741713c8906be', 'text': '• Provides logging and charging the API invocations', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 303, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b0ca45058e47248e0264fdc56ff7f3b6', 'text': '• API Exposing Function (AEF):', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 303, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '618dbec42193cd20b05d55021f542d60', 'text': '• Validates the authorization and provides the service to the API invokers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 303, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b57261e9eac6290c1ac71caa182a2f6d', 'text': '• Logs the invocation on the CCF and requests charging for the service', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 303, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f6384a901ac1fb5965a16eadfd99d07', 'text': '• API Invoker:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 303, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c73ca8416142c2d60f373499d7841e98', 'text': '• Discovers the service APIs from the CCF', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 303, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '56125292b2f339533cf25427c20b34f5', 'text': '• Seeks authorization for API invocations', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 303, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f1c11400a396658e7569cc22d59adc48', 'text': '• Avails the services provided by AEFs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 303, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0a561806eeda14d4da823390a89db346', 'text': 'The CAPIF functional model can be adopted by any 3GPP functionality- providing service API. In the functional model, API invoker within the PLMN trust domain interacts with the CAPIF via CAPIF-1 and CAPIF-2. The API invoker from outside the PLMN trust domain interacts with the CAPIF via CAPIF-1e and CAPIF-2e. The API-exposing function, the API-publishing function, and the API-management function of the API provider domain (together known as API provider domain functions) within the PLMN trust domain interacts with the CAPIF core function via CAPIF-3, CAPIF-4, and CAPIF-5, respectively. The CAPIF framework by itself is not enough to mitigate the API attack vectors; the following security controls are recommended to secure the API communications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 303, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f15c48f7444d658e3d26a200a97da75c', 'text': 'EDGEAPP is a new activity that 3GPP has just initiated. The details of EDGEAPP are mentioned in the 3GPP Technical Report TR23.758, which identifies the key issues and corresponding application architecture and related solutions with recommendations for the normative work.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 303, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7cfa4eb40e5bc5bb478deb4cf5040a29', 'text': 'Figure 5-43 shows the application architecture for enabling edge applications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 303, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ef150559d62267901c10f2dc890a5a4b', 'text': 'Application Edge Clients Application EDGE-7 Servers L EDGE-1 3GPP Edge Enabler Network EDGE-2 Server Edge Enabler Client EDGE-6 EDGE-4 Edge Data Network EDGE-8 Configuration Server', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 304, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5c13cb4ed4a44e5e236dfdefcc2d710f', 'text': 'Figure 5-43 Application Architecture for Enabling Edge Applications (Source: 3GPP TR 23.758 V17.0.0)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 304, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '659b78050ec97e8a6fe18a42b1089be7', 'text': 'Although the EDGEAPP architecture is at a very early stage, the key security requirements are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 304, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5092124798b8e0da52bd39c90e32afb7', 'text': '• The edge-enabling application architecture shall provide mechanisms for the mobile network operator to authorize the usage of edge computing services by the UE.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 304, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '04c7400f5fb47d1a01bf5244bd63ebe7', 'text': '• The edge-enabling application architecture shall provide mechanisms for the mobile network operator to authorize the usage of edge computing services by the edge application servers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 304, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c31c30e733a6519c1202f6d0ef690dc7', 'text': '• Communication within the edge-enabling application architecture shall be protected.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 304, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a204275429733c88b952f8d72f936d31', 'text': '• The authentication and authorization for the use of edge computing services shall support the deployment where the edge enabler functional entities providing the edge computing services are in the same or different trust domains with the 3GPP system.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 304, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4f2ec42ba9128ef726ef26ecc86b2c68', 'text': '• The edge-enabling application architecture shall support the use of either 3GPP credentials or application-specific credentials for different', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 304, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '79c929b68c1b6f679d213b3e7662f7af', 'text': 'deployment needs, for the communication between the UE and the edge enabler functional entities providing the edge computing services.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '35386ff0ae38c036ffc1c26dc30c4a8e', 'text': '• The edge-enabling application architecture shall support mutual authentication between servers (the Edge Data Network Configuration Server and the Edge Enabler Server, the Edge Enabler Server, and the Edge Application Server).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1efd158ce29ad4b40d0a4162d12bb1d1', 'text': '• The edge-enabling application architecture shall support authentication between clients and servers to support edge-enabling service authorization.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67ebc6a81170a185f0956e24eace2ccb', 'text': 'Apart from the studies being conducted by 3GPP on optional features, it is recommended that the service providers and enterprises using MEC applications use API gateways/API firewalls and follow best practices to secure APIs. The API gateway can be used as one method to mitigate the API attacks. The API gateway should have the following capabilities to protect the 5G applications and network functions from API-based attacks:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '49ef028498ba18ad12274606c9089613', 'text': '• Review all API responses and adapt them to match what the API consumers really need', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0f488ac5f5069f0bd7ec9e679196b907', 'text': '• Should allow definition of schemas for all the API responses and error responses', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7f0785eb0f8cf8967949f2830cf2d2ac', 'text': '• Enforce response checks and server-side data filters to prevent accidental leaks of data or exceptions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '57220a733a376e4f56b22932550d7768', 'text': '• Authorization checks with user policies and hierarchy', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3b32ed91de6fefd4cc969723a5420232', 'text': '• Check authorization for each client request to access database', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0362b269c1071b2ab4bff11fb52ad1c9', 'text': '• Check multiple ways to authenticate to APIs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'abbcb75ad99c4318dc8b7b51dbe67315', 'text': '• Be able to use standard authentication, token generation, password storage, and multifactor authentication (MFA)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '03056b86bd216640615fa1612c20fad2', 'text': '• Be able to filter server-side data', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '19c0a87623c931623218c11ead801e96', 'text': '• Enforce usage of short-lived access tokens', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '42814291f63ed1ba9896137bb44f7ef1', 'text': '• Allow authentication of MEC applications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '279bb70adbed4d81408ef971308cb1d7', 'text': '• Allow use of stricter rate limiting for authentication and implement lockout policies and weak password checks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2f57a920e1d0dcf3e71e44e1e462ffb4', 'text': '• Allow restriction on administrative access', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 305, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd8309fd803d9148b892054a3c4197b0b', 'text': '• Define and enforce all outputs, including errors', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7767d4c2ee8b4d3b5eff7cab06410961', 'text': '• Validate, filter, and sanitize all incoming data', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b17182b49ede81db4165be73a9a8bd6c', 'text': '• Define, limit, and enforce API outputs to prevent data leaks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '26e33bff0424df763976237e316c5120', 'text': '• Allow rate-limiting enforcement to match what API methods, clients, or addresses need or should be allowed to get', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '10ec96f9ae67bcbb6289619b14aecb58', 'text': '• Enforce rate limiting', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9873ebf8d21c2682c80834777abc9ff7', 'text': '• Enforce limit on payload sizes', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aeb8f3f66c7f9460986dc384cc462c58', 'text': '• Add checks on compression ratios', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2d818cc12fbe159d9374a49529d4bac', 'text': '• Deny all access by default', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '92b2130704608aa5604a04fa4226ad07', 'text': '• Only allow operations to users belonging to the appropriate group or role', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3638f24509414c50b2f32e15a1cee5ce', 'text': '• Do not automatically bind incoming data and internal objects', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '293b058623023311d52da5c5d8c37aaa', 'text': '• Allow configuration of parameters and payloads', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3290687dd452e01f5560ac5651fed638', 'text': '• Allow enforcing specific schemas for runtime', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7989db8b6d9fd1d7a282a91b7e51ef86', 'text': '• Strictly define all input data, such as schemas, types, and string patterns, and enforce them at runtime', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8020cd68feadff07d58d218dccd8c134', 'text': '• Integrate with SIEMs and other dashboards, monitoring, and alerting tools', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd6370868110ad55df94c450132ae0875', 'text': 'Apart from the security controls provided by API gateway/API firewall, the following best practices will enhance the security of the APIs:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9394eedbff86ed80f7c94f583c69bed0', 'text': '• Properly documenting all functions and software development kits (SDKs)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6ffa40d56d77e540a41a0a3a4b7424ff', 'text': '• Enforce authentication and authorization access by integration with IAM (Identity and Access Management) solutions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b10c0670da97fafb5901cfaf045e106d', 'text': '• Use RBAC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2f475ddc9f6e1c98b702ee4f076fff12', 'text': '• Use access policy that denies all access by default', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c59713556e77d15650d48cfa56be844f', 'text': '• Audit the API implementation at least every 3–4 months, along with an audit whenever a new MEC application is deployed', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '35807debf5cc095fa375bd26be8c2619', 'text': '• Configure maximum resource usage by a container', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7613a6981ded0a943686e0a23a77626f', 'text': '• Prevent the use of personally identifiable information (PII) and any non- public information', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3793a32b61b23e76965f925c81309dff', 'text': '• Use segmentation to segment production and non-production data', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 306, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '11e025bbdcc278438eb14426f0d72a87', 'text': '• Ensure MFA and strict access polices are implemented', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ba210c2125f70d1b4ecf59969db85c0d', 'text': '• Properly design and test authorization', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eddea4da986071c16e16a0d3bae38110', 'text': '• Ensure secure hardening and patching processes for all MEC applications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7f7a2628c550838bbce3076aba13eb3c', 'text': '• Automate locating configuration flaws', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd208662b67c964945a24d3d3c5ab8774', 'text': '• Disable unnecessary features', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4ebbb2b09264d482364700d804038acb', 'text': '• Keep an up-to-date inventory all API hosts', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3c6c924664f5a34845feca73f87d4dc5', 'text': '• Restrict use of old versions of APIs or backport security fixes to them', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'abc3dc9a0f77a51cafeaa09072128fcc', 'text': '• Implement additional external controls, such as API gateways/API firewalls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2e33ff0ca5171a2ba52c2c0c7e52ae4d', 'text': '• Log failed attempts, denied access, input validation failures, or any failures in security policy checks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5884e0ff999e21cf7a878d2445293ef4', 'text': '• Ensure secure storage of logs as logs might have sensitive information', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a38c9777fbd4fbad82021d8d65b9140', 'text': 'Figure 5-44 shows the mitigation of a threat attack surface from API injection attacks using an API gateway/API firewall.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '1da920c46111f71ced529695ac487af7', 'text': '. - ervice PM \\ N / | §WC9 CM S P Pod j=s=) App App API Gateway ~~~~~ G = fommmmmeaaa v Service Service FM Analytics Attacker Pod App Identity & Authentication, Authorization', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '95bda0dce2179f23ebe5f391ca830e4d', 'text': 'Figure 5-44 Mitigation of API Injection Attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '01c3c350a82575c555204c68c88f825e', 'text': 'Figure 5-44 shows an example of mitigating the API injection attacks in the 5G MEC deployments. The attack vector in this example is due to the credentials', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 307, 'parent\_id': '95bda0dce2179f23ebe5f391ca830e4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e6c5bfc850509257196633233bf9322c', 'text': 'of the server being exposed a weak device interacting with the MEC application. This credential is then used by the attacker to exploit the weak API security controls on the 5G MEC and obtain sensitive data from the MEC application database. If we look at the threat surface for this attack, it is multi- dimensional and would require security best practices to be followed along with deploying API security controls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 308, 'parent\_id': '95bda0dce2179f23ebe5f391ca830e4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '449da54aab2635b9ed4039857cd6e2c2', 'text': 'To mitigate attacker obtaining credentials of server from the weak device and mitigating the API injection attacks, the following best practices need to be followed:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 308, 'parent\_id': '95bda0dce2179f23ebe5f391ca830e4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f904ab5dc6a1bc4039117802b0d4b93b', 'text': '1. Ensure that the credentials of the server are not exposed. This requires the devices interacting with the MEC application to have strong access control mechanism and not allow any unauthorized user to access the devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 308, 'parent\_id': '95bda0dce2179f23ebe5f391ca830e4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ebb1d8a2ca3820a68c908dd14d33504c', 'text': '2. If the credentials of the server need to be stored in the device, then it should be accessed only by authorized users having the right level of privilege and depending on the type of the device, it is best stored in a secure encrypted non-removable storage within the device.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 308, 'parent\_id': '95bda0dce2179f23ebe5f391ca830e4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '812becba9de9e8e98c61db53be28ff76', 'text': '3. The user and the device should be authenticated (who the person is) and an authorization (what the person can do) mechanisms should be applied to ensure that the user is restricted to limited set of API calls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 308, 'parent\_id': '95bda0dce2179f23ebe5f391ca830e4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed26acd76bdfb81bf291f0ff8d920cba', 'text': '4. Authentication and Authorization mechanisms should be applied at each request/as often as possible', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 308, 'parent\_id': '95bda0dce2179f23ebe5f391ca830e4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8c28e248acedd2ff2b6507709597a4e9', 'text': '5. Ensure having server-side input validation as well as client-side validation. Client-side validation is easily bypassed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 308, 'parent\_id': '95bda0dce2179f23ebe5f391ca830e4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3dd580f32001379cd7c673722f2b4262', 'text': '6. Ensure using parameterized queries instead of string concatenation with the query. Having parameterized query restricts the input of the API user to specific type of individual parameters and prevent the API user to input entire SQL statements intentionally or unintentionally.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 308, 'parent\_id': '95bda0dce2179f23ebe5f391ca830e4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '574372e8ea9e52512a1476afe0c70a4c', 'text': '7. The input validation should also be carried out at different layers, as an example in the GUI (Graphical User Interface) – if GUI is used, MEC application data validation if the API query is directed towards the application and database data validation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 308, 'parent\_id': '95bda0dce2179f23ebe5f391ca830e4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd4fcecb48139247736768d07f5ec1f84', 'text': '8. Conduct regular audit and penetration test of your API deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 308, 'parent\_id': '95bda0dce2179f23ebe5f391ca830e4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c801a3ca52e227d67b95565d3b2cf5b6', 'text': 'Figure 5-45 shows the mitigation mechanism for the attack based on excessive data exposure using an API Gateway.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 308, 'parent\_id': '95bda0dce2179f23ebe5f391ca830e4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c5361dd46ecb018f1501cdfd0165b341', 'text': 'MEC application hosted on Public or Private cloud of Enterprise or Service Provider', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 309, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '9ac60ce5f9d17f4db0dd2f0982110739', 'text': 'MEC application hosted on Public or Private cloud of Enterprise or Service Provider - C onfig data 7 Storage /Cache = \* M2M device inventory A v To NEF M2M Application A l Fllterlng pollcy S AF’I Identity, Authentication, Gateway Authorization li Attacker User', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 309, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd99403d7ff1e2dc59c52e3e22722d174', 'text': 'Figure 5-45 Mitigation of API Excessive Data Exposure Attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 309, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4d47285021a4e4e228506555cac946ed', 'text': 'In 5G, the MEC applications can be used for a variety of use cases. Many of the use cases can be for the public sector, defense, and healthcare sector. The database of MEC applications aimed at these critical use cases might hold very important data that should not be exposed. Many developers program APIs with simple codes that rely on clients to perform filtering without much consideration given to security for extra checks on the API request or response messages. In the majority of the instances, the programmers do not realize the sensitivity of the data being transferred. As shown in Figure 5-45, the following mitigation mechanisms can be used to identify any excessive data exposure and mitigate it:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 309, 'parent\_id': 'd99403d7ff1e2dc59c52e3e22722d174', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aaeaed3345e9b4f0ed47ce2b6cbc587e', 'text': 'Step 1. This step should always be the authentication and authorization of the user and device. Device authentication and authorization policies are important in the M2M use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 310, 'parent\_id': 'd99403d7ff1e2dc59c52e3e22722d174', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fafc5532c74ff18158a0f8d3c2b4b48e', 'text': 'Step 2. Ensure the right filtering of the data within the API response. This is to ensure that the response of the API call is only for the requested data and that excessive and sensitive data is not exposed. For the right filtering to take place, it is necessary that the API gateway include the policies for API requests, API response, and the error codes. As 5G network functions and MEC applications would communicate mainly using the REST API, filtering policies should be applied as a mandatory feature in any 5G MEC application being deployed by the service provider/enterprise to limit any exposure of sensitive data and mitigate any data being exfiltrated and hoarded by the attacker.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 310, 'parent\_id': 'd99403d7ff1e2dc59c52e3e22722d174', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '408c87398653e782e4568e634dc80a45', 'text': 'Figure 5-46 illustrates a method of applying filtering policies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 310, 'parent\_id': 'd99403d7ff1e2dc59c52e3e22722d174', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a73d567ff4ad27ff4c599ddcef43f3d4', 'text': 'MEC application hosted on Public or Private cloud of Enterprise or Service Provider', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 311, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '9415f51faab273cdfd5acae84ac8af82', 'text': 'MEC application hosted on Public or Private cloud of Enterprise or Service Provider Response includes info of all devices such as : “devicename”: device1 + Config data “deviceid”: 1d25a164771006197fd + Storage/ Cache ‘power output” 10mW 8 ‘ip address"10.10.10.11 + M2M device inventory ‘address”:1 Main street, Swords, Dublin [ ———— Fp—. “username”abed @hotmail com o ‘password""abed1111" ToNEF MM Application \'“devicename": devicel10 “Ueviceid" 7f31a74d113fc192df1d ‘power output”:10mW UPF Fitering policy ‘ip adalress”10.10.10.111 ‘address"”1 seatown, Swords, Dublin “Username"abcd @hotmail com ‘password""abcd1211" [dentity, API Authentication , Galeway Authorization Policy filters AP! response output to the below: devicename\'”: device “deviceid”: 1d25a16a771cc6197d ‘power output 10mW Excessive data exposure .= prevented - only basic atribute deviceidinfo: device1 4 values are retumed for the AP “deviceid": 1d25a160771c061971d = Query User ‘Dower output”: 10mW', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 311, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'text': 'Figure 5-46 Applying Filtering Policies to Mitigate Excessive Data', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 311, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '99071a3808b45ec46304e7dae6a7b2d5', 'text': 'Exposure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 311, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e783d950b78d69af94b9add70409662f', 'text': 'As shown in Figure 5-46, a method of mitigating excessive data exposure is to use the right filtering policy and is indicated in the following steps:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 311, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b0de0a844eaf9c84c68cbeb7df52d45a', 'text': '1. The user or an attacker issues a query using an API GET request for getting the information for device1.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 311, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '006048f26cad865df182ae5fe60bd151', 'text': '2. The checks are carried out for authentication and authorization.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 312, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '98c20c07098229070347eac2c90977c7', 'text': '3. Once the authentication and authorization checks are successful, the API query is sent toward the MEC application database.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 312, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ec57e7b257b1f7c4754e0afc42d8c5e1', 'text': '4. The MEC application database, which holds the configuration data and the storage and device inventory then responds with all the device info, which includes sensitive data such as device IP address, username, passwords, and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 312, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a96b085085755eced7fab236fc403f70', 'text': '5. The service provider/enterprise vertical deploying the MEC application also includes a filtering policy to ensure that only nonsensitive data is allowed to be exported. This can be achieved by carrying out checks in the “attribute: value” pairs and restricting certain attributes to be exported. The filtering policy is an API gateway functionality provided by a few API gateway vendors today. If you have an existing API gateway that does not support this function, you can use an intrusion prevention system (IPS) or a firewall to carry out the aforementioned attribute value checks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 312, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e6f93336b78adf2bac5f274f892fb709', 'text': '6. Depending on the filtering policy applied, only nonrestricted attributes are allowed to be exported. In the example in Figure 5-46, only the attributes “devicename”, “deviceid”, and “power output” are allowed to be exported, thereby preventing sensitive attributes such as “ipaddress”, “address”, “username” and “password” from being exported.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 312, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5b3a7c9abf3f4d06d78105ee33ddc9d1', 'text': '7. The user or the attacker now receives only the nonsensitive attributes, and excessive data exposure is avoided.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 312, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dd7c9ef809203a3b7ec48e5f2d92c4c3', 'text': 'It has to be noted that varying numbers of MEC applications can have different levels of sensitive information in the attribute values, and where the attribute is present depends on the Managed Object Model of the device. For some MEC applications, even the “deviceid” might be sensitive information. So the filtering policy needs careful consideration and should not be a generic deployment of rules; it should be considered on a case-by-case basis and audited regularly, at least every 3 to 4 months and each time a new MEC application is deployed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 312, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e30b8a850396c3f1e6deb226558d5b4b', 'text': 'In another variant of the attack, the attackers can exploit MEC applications that are vulnerable to Broken Object Level authorization by manipulating the ID of an object that is sent within the request. An example of this follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 312, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ec93949e31485cfacdc366fdee11f095', 'text': '• Intended use: GET/MEC\_application/user/personal\_info', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 312, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bb576b7ad8169a4f705b0194b2517353', 'text': '• Manipulated use: GET/MEC\_application/adminuser/personal\_info', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 312, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3cc249812bdcfabf6f25204dae736854', 'text': 'Here, attackers have substituted the ID (user) in the API call with an ID belonging to another user (adminuser) to exploit the MEC application. The attack is carried out by an attacker observing the pattern of the API call and then inserting certain ID values by guessing and modifying the IDs. This issue is extremely common in API-based applications because the server component usually does not fully track the client’s state and instead relies more on parameters like object IDs that are sent from the client to decide which objects to access. Generally, the application developers do not include code to have proper authorization checks, allowing attackers to access sensitive information related to another user or information related to an admin user and then launch a privilege escalation-based attack on the network. The attacks can also be launched to delete or modify certain information that might lead to service outages and loss of revenue for the entity providing the services related to the MEC application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 313, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '05af786e72823a5b926fc576f0b9359e', 'text': 'To mitigate the attacks based on Broken Object Level Authorization and user authentication, it is important to have granular access and authorization controls implemented in the MEC application deployments to ensure that sufficient checks have been carried out on the access rights of the user. The ID within the API should also be masked and shouldn’t be easily guessable.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 313, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '71e65affab773a24da9f183df0ef0ff9', 'text': 'Figure 5-47 shows an example of one of the methods of mitigation of threats based on Broken Object Authorization. In this example the M2M application developer has ensured that the M2M application database has included the user-to-object access checks to ensure that the user can access or query the objects within the database. Using the object access checks will also mitigate the attack vector whereby an attacker tries to use the name of a legitimate user with incorrect credentials. However, if the attacker has the correct username and the related correct credentials, they can have an unauthorized request using the API calls. This can be mitigated by using MFA security controls, which allows access to the users after multiple layers of authentication to verify the identity of the user accessing the API.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 313, 'parent\_id': '9ae4df9eb0d30f2abddaed5b030a7086', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f3caa5ee359b09164524072c9bcac439', 'text': 'MM Application Access Logs MM Application Brian is not allowed to access Database the object ‘personalinfo”! 0 e ® Reject message and error code stored = object read object info read info modify modify Is Brian permitted to access Request from Brian: REJECTED the object ‘personalinfo”? Paddy v v v v GETIM2M\_application/user/personalinfo Niamh v v ) X Brian v X X X <« Brian’s a valid user and s authenticated Identity, Authentication, API Authorization Gateway Request from Brian: GET/M2M\_application/userpersonalinfo f User / atlacker', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 314, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'abe8c8b833d8f558495b00057629d249', 'text': 'Figure 5-47 User-to-Object Access Checks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 314, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '659288734e286f96bbdca5a2dbadfd75', 'text': 'Figure 5-47 illustrates one of the methods for mitigating a Broken Object Authorization–based attack, which is explained further in the following steps:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 314, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4a034d9cf1cc805eb842a34c0bad0fcc', 'text': '1. The user sends an API GET request for user personal info. In this example the name of the user is Brian.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 314, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '511b55b0f9c7ba69c303bf805e7174b9', 'text': '2. An authentication and authorization check is carried out to check whether Brian is a valid user.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 314, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '81a1b207b735e8aaf449e2fb1026c7e3', 'text': '3. The user Brian is authenticated and the GET request is sent toward the M2M application database.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 314, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0b7ae4b301245605aee5baf9faf53fc2', 'text': '4. The database queries the user-to-object access mapping table to verify if the user Brian is allowed to access the object personal info.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 315, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '050523a6dccb3d00693d1d466fc38847', 'text': '5. The user-to-object access rules are checked to verify the access rules. This is the critical step which should be included for verifying the API request and verifying the authorization rules as to what object the user is allowed to access.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 315, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1cba224c648de68efc179911e0148b26', 'text': '6. It is confirmed that the user Brian cannot access the user-to-object access mapping, and Brian is not authorized to access the requested object.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 315, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'effc670a4dedfb7b42f0f0bad95c2e2a', 'text': '7. The request from Brian to read the attribute value is rejected and the requested information is not passed on to Brian. An added step that could be optional in this process could be a reply with error code.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 315, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '71205a8955b6454ab9580b3a45431e81', 'text': '8. The rejected request from Brian is logged into the M2M application logs, which can then be used by the monitoring entity or security operations center (SOC) to further investigate the activity.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 315, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'fdecece816c37aef9dcd4ae996d04881', 'text': 'Validating Both Read and Write Requests', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 315, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '97c586e5a2e4e8174e7d46f9269a633e', 'text': 'Another technique to mitigate API vulnerabilities based on Broken Object Authorization is to validate the read and write request. Here, the user/attacker tries to use the DELETE API request to create or update the resource or attribute.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 315, 'parent\_id': 'fdecece816c37aef9dcd4ae996d04881', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b6615acc723ecda2ca10e8d0e6fe16bf', 'text': 'Figure 5-48 shows another example of mitigation of Broken Object Authorization–based threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 315, 'parent\_id': 'fdecece816c37aef9dcd4ae996d04881', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c367cb300566b93ace05b952bc5ac772', 'text': 'M2M Application M2M Application Brian s not allowed to delete Access Logs . Database the object ‘personalinfo”! Reject message and error code stored = ﬁm% =" Seeeaan object read object info read info modify modfy »x Request from Brian: REJECTED [s Brian permitted to modfy or Paddy v v v v DELETEM2M\_application/user/personalinfo delete the object ‘personalinfo”? amh v v X X Brian v X X X Brian s a valid user and s authenticated Identity, API Authentication, Authorization B Gateway Request from Brian: DELETE/M2M\_application/userjpersonalinfo : User / attacker', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 316, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'be348805c7dc2ec78746d10222b43752', 'text': 'Figure 5-48 Validate Read and Write Request', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 316, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd2623cfc282fa2c99e610020fe945e6e', 'text': 'Figure 5-48 illustrates another method for mitigating Broken Object Authorization–based attacks, which is explained further in the following steps:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 316, 'parent\_id': 'be348805c7dc2ec78746d10222b43752', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ab49ba383988acd9df0374b27dd464b4', 'text': '1. The user sends an API DELETE request for deleting user personal info.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 316, 'parent\_id': 'be348805c7dc2ec78746d10222b43752', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7910d817610ea9b50ceefe5cbfad4fd0', 'text': '2. The authentication and authorization check is carried out to see whether or not the user is valid.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 316, 'parent\_id': 'be348805c7dc2ec78746d10222b43752', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '428f134e200a6e72d180c70b2e8be319', 'text': '3. The user is authenticated, and the DELETE request is sent toward the M2M application database.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 316, 'parent\_id': 'be348805c7dc2ec78746d10222b43752', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '148a29930b65e4b889f9c4d003019709', 'text': '4. The database queries the user-to-object access mapping table to verify if the user Brian is allowed to modify or delete the object personalinfo.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 317, 'parent\_id': 'be348805c7dc2ec78746d10222b43752', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6f185ce44b0925c17f62b38ba292074b', 'text': '5. The user-to-object access rules are checked to verify the access rules.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 317, 'parent\_id': 'be348805c7dc2ec78746d10222b43752', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5b214e6e748c6d0937ff5d43f5ef49e0', 'text': '6. It is confirmed that the user Brian cannot modify or delete the user-to-object access mapping and Brian is not authorized to access the requested object.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 317, 'parent\_id': 'be348805c7dc2ec78746d10222b43752', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f0a5804004c859165dccd454c63c510b', 'text': '7. The request from Brian to delete the attribute is rejected and the deletion action is not varied out. An added step that could be optional in this process could be a reply with an error code.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 317, 'parent\_id': 'be348805c7dc2ec78746d10222b43752', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b9c67ea0ba86a4a879323d3e27fa9925', 'text': '8. The rejected request from Brian is logged into the M2M application logs, which can then be used by the monitoring entity or security operations center (SOC) to further investigate the activity.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 317, 'parent\_id': 'be348805c7dc2ec78746d10222b43752', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '632b80337f553315162efb7b00d2d74a', 'text': 'DDoS Protection', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 317, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9b104ae07c72dd3a3660b364d4123e89', 'text': 'In order to properly secure the “full stack” in the MEC layer that delivers a connected application, two fundamental elements can be applied: visibility and control. Visibility refers to the ability to see and correlate information from the carrier cloud to baseline proper behavior and then to measure deviation from that norm. Simply said, “If you can’t measure it, you can’t manage it.” Sources of visibility come from traditional network measurements (NetFlow, open flow, and so no), but the need to measure all aspects of a flow, from all elements of the carrier cloud to the application to the end customer, has changed what data is collected and where we get it.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 317, 'parent\_id': '632b80337f553315162efb7b00d2d74a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a6d115817daddc3d642f236925065d67', 'text': 'Cybersecurity vendors are now providing enhanced visibility, which includes the use of application-level probes that are synthetically generated and travel through the network to get a clear picture of how an application is behaving. Another example is where the Path Computation Element, which has a near real-time database representing the network topology, is queried programmatically to determine the impact of a potential mitigation action on critical service classes for DDoS. Once all of the telemetry is gathered, a security controller and workflow will analyze it and determine, based on policy, suggested mitigation and controls to be applied. Of course, we have an iterative loop of constant learning.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 317, 'parent\_id': '632b80337f553315162efb7b00d2d74a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fe149f380af6813db9c69f2110d7ccb7', 'text': 'For determining the anomalous traffic, the DDoS protection solution would normally baseline the network by monitoring for a couple of weeks. This baseline would help the DDoS protection solution understand what traffic', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 317, 'parent\_id': '632b80337f553315162efb7b00d2d74a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '205dceeacd24b7dcb1035908849a2f16', 'text': 'pattern can be considered normal and what traffic patterns should trigger the activation of DDoS mitigation steps.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 318, 'parent\_id': '632b80337f553315162efb7b00d2d74a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8845b8650b471a06b5197c3468493af7', 'text': 'Depending on the MEC deployment model, an option of on-premises, cloud, or hybrid DDoS protection could be used. The key is to have an effective security architecture that includes effective DDoS protection. To have effective DDoS protection, it is important to have an IP protection database and a strong threat intelligence input to the DDoS solution, primarily to minimize any chances of increased frequency of zero-day attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 318, 'parent\_id': '632b80337f553315162efb7b00d2d74a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '51696a1d2a277a6b5f9fde00e0fccb3f', 'text': 'There are different approaches to DDoS attack mitigation; the key approaches are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 318, 'parent\_id': '632b80337f553315162efb7b00d2d74a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e7c4f1839244c9e7875aff9a1efc4652', 'text': '• On-premises: When on-premises mode of DDoS protection is chosen, service providers and enterprises benefit from an almost real-time and automated DDoS attack detection and mitigation. Within seconds of the start of an attack, the MEC deployments are protected. On-premises mode of the DDoS solution, though effective, becomes less effective when a large-volume DDoS attack is launched, as an on-premises DDoS solution is normally deployed based on the DDoS traffic volume, which needs to be mitigated. The larger the volume decided during deployment, the higher the cost. As a rule of thumb, many DDoS vendors recommend the DDoS traffic mitigation volume be around 30–40% of the inbound traffic. This makes on-premises anti-DDoS solutions more favorable to be used against application-level DDoS attacks. Due to the high volume of the DDoS traffic in volumetric DDoS attack scenarios, cloud and hybrid anti- DDoS solutions would be more effective in mitigation, as compared to on- premises DDoS solutions, which are limited in the volume of DDoS traffic that can be mitigated.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 318, 'parent\_id': '632b80337f553315162efb7b00d2d74a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9d92e5ff7383ceb7738d6a973a879c26', 'text': '• Cloud: When cloud mode of DDoS protection is chosen, it is mainly aimed at mitigation of the DDoS attack and not so much as the detection part of the DDoS solution.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 318, 'parent\_id': '632b80337f553315162efb7b00d2d74a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '956191d88cc8431e1ff100e54cbed343', 'text': '• Hybrid: Hybrid DDoS solutions offer the best mitigations by combining advantages of the on-premises and cloud deployments of the DDoS solution. Attack detection and mitigation start immediately using the on- premises mitigation device, and the cloud deployment caters for the mitigation by diverting the traffic to the cloud, where it is scrubbed before being sent back to the service provider or enterprise. To have an effective mechanism of DDoS protection, it is recommended to have a tight', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 318, 'parent\_id': '632b80337f553315162efb7b00d2d74a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '027f880e9eb62be91258e7a8fd50e370', 'text': 'integration for information exchange between the on-prem and cloud- deployed DDoS solutions to enhance the DDoS attack mitigation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 319, 'parent\_id': '632b80337f553315162efb7b00d2d74a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '03040afa2019643e7a04c523cb2381ef', 'text': 'Some DDoS attacks also require a web application firewall (WAF). WAF would protect the network from application layer attacks such as SQL injection. WAF would normally be deployed between the Internet layer and the application layer and analyzes the HTTP communications. For mitigation of DDoS attacks, WAF could be deployed for managing an IP reputation database that tracks and blocks malicious traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 319, 'parent\_id': '632b80337f553315162efb7b00d2d74a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '49ad445bab31392a8c800a31198e3e11', 'text': 'Figure 5-49 shows an example of DDoS protection against HTTP attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 319, 'parent\_id': '632b80337f553315162efb7b00d2d74a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '110c91d1eb04c923fa0f989caa4ea86d', 'text': '0 Attacker a —» Legitimate traffic ---% DDoS traffic SP loT Applications & Internet 1 | | ] Y Y | X : X i X | \\ DDoS Protection & WAF Legitimate inbound Y Y Y traffic from internet oW ¢ [ Legitimate user Legitimate User can o ! access MEC application =] MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 319, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bbf4e4a40fcb8f98c0fc1273c3491be1', 'text': 'Figure 5-49 DDoS Protection Against HTTP Attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 319, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c52fb655810fe4a665f0464f902e6110', 'text': 'As shown in Figure 5-49, inbound DDoS attacks could be mitigated by using DDoS protection using anti-DDoS and WAF between the Internet/web layer and the MEC layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 319, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5f9fbed86af15e7af41cd035e4478db6', 'text': 'In this attack vector, the attacker aims to cause DoS for the MEC application users by using a form of HTTP flood attack. Here, the aim is to overwhelm the MEC application with HTTP requests mostly with the help of bots, which makes it unable to respond to legitimate user requests.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 320, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dae78ff06188400dd25101993605a597', 'text': 'The mitigation of the HTTP attacks requires sophistication, as the aim is not to drop all the HTTP requests because there would be legitimate requests to and from the MEC application that should not be blocked. The mitigation of such attacks would require a multilayered security control. One of the security controls used is a DDoS protection solution that has WAF capability. The service provider/enterprise can now selectively allow only legitimate traffic to communicate with the MEC applications, while the rest of the DDoS traffic can be blocked or sent to a DDoS scrubbing center for more analysis.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 320, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6a34355d4447afabc22d2784865b5992', 'text': 'Figure 5-50 shows another example of mitigating the DDoS attacks on the MEC application deployed on the public cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 320, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '23d846d96b44151660105a5a3c8af520', 'text': 'S — [ X A - DDoS MEC Attacker . 0F Application F ——— MEC services deployed in public cloud Intemet / Public cloud > A [ A - B @AF) L | i A gNB i s i B Devices using MEC MEC - Compute & storage application', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 320, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9889df5370af2b4eae754369804695aa', 'text': 'Figure 5-50 Multilayered Security Controls to Mitigate DDoS Attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 320, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7499526f7fb639aa1b20bcde928d9d30', 'text': 'As shown in Figure 5-50, in this MEC deployment model, the MEC applications are deployed on the public cloud and the storage and compute are deployed on the on-premises infrastructure of the service provider/enterprise. The security controls considered for mitigating the DDoS attack surface are vulnerability assessment, patch management, enhanced visibility, an anti-DDoS solution, and a threat intel mechanism with artificial intelligence (AI) and machine learning (ML) to proactively detect threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 321, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1341bd2a549fd2b002c37aad46b6a22f', 'text': 'There are many variations in the way that the MEC applications deployed in the public cloud could be attacked. The attack vector example in the diagram is due to vulnerabilities in the application deployed in the cloud, which is exploited by the attacker. The application vulnerability might be due to many open source components used to create the microservice. This is of particular interest in 5G, as many of the applications being deployed in 5G will be “CNF created” by using open source components. These open source components might have vulnerabilities not yet patched or widely understood. These vulnerabilities are then exploited by the attacker or attacking entity to cause DDoS or DoS for legitimate users. In Figure 5-50, the devices using MEC applications cannot be served by the application deployed in the cloud due to the attacker consuming the resources of the application by overwhelming it with “fake” requests.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 321, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e2b2a4fb937d03935f173d483beea039', 'text': 'To mitigate these kinds of DDoS attacks, it is recommended to follow a baseline security control and process, as described in the list that follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 321, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b86e45c24f71723f004f4f40741248dc', 'text': '• Deployment of an MEC application specific to 5G use cases should have a vulnerability assessment system in place that checks the applications for any vulnerabilities and patches that can be applied to mitigate the vulnerability. The vulnerability assessment should include the MEC applications deployed in cloud and on premises.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 321, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1668e5e5a7f5c008f276523f8a93da2d', 'text': '• There should be an enhanced visibility layer providing visibility at the application level, such as application-to-service mapping. The service could include DNS for NTP, which is being used by the application. A baseline should be created to understand the normal behavior of the application, including the memory being consumed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 321, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd670bae6b5f529812208e8886c212f26', 'text': '• The critical applications serving important use cases such as government, defense, utility sector, and so on should have enhanced visibility and alerting procedures. An example of enhanced visibility layer is to determine if there is any malicious traffic in the encrypted communication between the web and MEC application catering to the critical use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 321, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '60ca3d9d7e5343602c2753e9c2acb006', 'text': 'As shown in Figure 5-51, the communication between the MEC application deployed in the cloud and on premises could have different modes of communication. Some could be based using API calls, and others could be non-API calls. The API messages could be secured by using HTTPS. To secure non-API communication, IPsec is recommended.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 322, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '800082fa6dd2d8d68f2147d5d33ebcc9', 'text': 'MEC off-prem @ Google Cloud aws /A Azure p— [\_APL\_X\_API | (Non - API] HTTPS< O IPsec [ AP API Non - API © & Gl [\_MECAppin | [(UPF ) Cu DU FW S — = MEC on-prem', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 322, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8e49ee7f7245fea5a4e4fd664c8b42d5', 'text': 'MEC on-prem', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 322, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2a3dde2d6d6d6a3d28fb006eb3771e8e', 'text': 'Figure 5-51 Securing API and Non-API Interfaces', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 322, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f6f449e6fd22995a99dd98debaf196c1', 'text': 'Using DDoS protection algorithms that employ AI and ML is important for detecting and proactively mitigating zero-day attacks. Instead of having the AI and ML restricted to DDoS solutions only, they should instead be applied to the threat intelligence layer, which can then be used as a threat intel for other security controls as well. This will help the end-to-end security architecture have better efficacy.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 322, 'parent\_id': '2a3dde2d6d6d6a3d28fb006eb3771e8e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '47c83a21d4c6aefe7cf5b41e11f7d416', 'text': 'All of the preceding methods described are effective if the attack has been seen before in other networks and there is a known mechanism to mitigate it. For', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 322, 'parent\_id': '2a3dde2d6d6d6a3d28fb006eb3771e8e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1aff026b460844e703e2494d2115e4c1', 'text': 'mitigation of zero-day attacks, however, there needs to be a bit more stringent security controls in place to ensure proactive mechanisms to deter the attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 323, 'parent\_id': '2a3dde2d6d6d6a3d28fb006eb3771e8e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '66744f302e0419acc72485a67cc1b163', 'text': 'One of the mechanisms to mitigate the zero-day attacks would be to follow a method to create a baseline of the network and then look out for any anomalies. Any traffic showing an anomaly should then be further analyzed to understand the nature of the traffic and then generate automated rules to block it if it’s seen again anywhere else in the network. The best practice of considering all traffic untrusted and then allowing traffic further in the network after going through mechanisms to trust it is very effective. DDoS mitigation mechanisms that can be deployed in the MEC or the edge of the network are very effective at mitigating DDoS attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 323, 'parent\_id': '2a3dde2d6d6d6a3d28fb006eb3771e8e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b75ce89d6fcd37ab25dbdb5c42100504', 'text': 'Real Scenario Case Study: MEC Threats and Their Mitigation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 323, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'de9d72d5ffeddad522f8001ec2b65129', 'text': 'The preceding sections describe the threats and mitigation techniques for specific areas of concern while deploying 5G MEC. This section focuses on a multidomain attack and discusses methods to deploy security controls at different parts of the infrastructure to mitigate the multidomain attack in a real- life environment. Although 5G was not widely deployed at the time of writing this book, this section is based on real-life attacks in similar environments or proof of concepts and lab tests done by various customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 323, 'parent\_id': 'b75ce89d6fcd37ab25dbdb5c42100504', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd08a2557bb67bf060f999a7c47e62f25', 'text': 'To explain the attack scenarios, an example of the MEC deployment, as shown in Figure 5-52, is considered in this section.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 323, 'parent\_id': 'b75ce89d6fcd37ab25dbdb5c42100504', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '1f025fc4a54660143e85f2733ffde3e7', 'text': 'DU connected to CU deployed in public cloud-hosted MEC CU, UPF, AMF , SMF MEC applications ] API MEC hosted in Public cloud (for low # latency use cases) & Internet OAM AMF , SMF, 4--- e ) (R P S ERE, NEF, NSSF, A PCF, UDM, At:l EEe = AUSF, UDM Centralized 5GC Public network 7 Containerized DU Private / Non-Public 5G stored in a low footprint Enterprise network connected to server in RAN site M2M devices DU, CU, UPF A centralized 5GC control plane MEC application functions using public network ( ). B ¢ ol Enterprise DC Enterprise MEC deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 324, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '863e43fb0aeca89f0044f45ed1c6a917', 'text': 'Figure 5-52 Example of 5G MEC Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 324, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bd6ba633da3fb543c7ade0f6a44e6452', 'text': 'As shown in Figure 5-52, the MEC deployment in this example consists of two layers of MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 324, 'parent\_id': '863e43fb0aeca89f0044f45ed1c6a917', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fac4692d074482eeff67e97745a5c0a6', 'text': 'One of the MEC options is realized by implementing it in the public cloud and hosts the CU and UPF, enabling URLLC use cases aimed at IoT devices and healthcare.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 324, 'parent\_id': '863e43fb0aeca89f0044f45ed1c6a917', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7ed3a5f6b3c73670d51be144c6c2dab4', 'text': 'In this deployment option considered by the service provider, the Radio Resource Unit (RRU) and the DU are deployed using a low-footprint server. The low-footprint server hosts the containerized DU, which could be open source or from a RAN vendor. One of the reasons a service provider might use the option of having a containerized version of DU deployed on the RAN site could be due to specific use cases that require extremely low latency and hardware acceleration, where certain computing tasks are offloaded to specialized hardware components. This mode of deployment is particularly helpful when Multiple Input Multiple Output (MIMO) and massive MIMO are', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 324, 'parent\_id': '863e43fb0aeca89f0044f45ed1c6a917', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b2b20b60e8f06bc4b816be590831d138', 'text': 'deployed. In some cases, even the CU is deployed on the RAN site, but it would limit the aggregation capability of the CU, put pressure on the scalability of the DU, depending on the server footprint, and needs careful consideration. As shown in Figure 5-52, the DU is configured to connect to the CU, which is implemented in the MEC hosted in the public cloud. Other components hosted in the public cloud MEC are the 5G user plane functions (such as UPF), 5G control plane functions, such as Access and Mobility Function (AMF) and Session Management Function (SMF), and MEC applications that would usually include the application configuration, storage, performance, and fault management.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 325, 'parent\_id': '863e43fb0aeca89f0044f45ed1c6a917', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e66e94940bd913019f3af6da6681b879', 'text': 'The second MEC in Figure 5-52 is implemented in the enterprise environment. It is based on private/non-public deployment of 5G, where the enterprise has deployed the RAN infrastructure, user plane functions of 5G, and the MEC application within the enterprise perimeter. Usually, the virtualized components, such as DU, CU, UPF, and MEC applications, would be a containerized form factor and deployed in the enterprise data center.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 325, 'parent\_id': '863e43fb0aeca89f0044f45ed1c6a917', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '352a137ec2656eef8988b8d4d248ca85', 'text': 'The control plane functions of 5G for the enterprise MEC deployment are located in the service provider’s data center and will host the AMF, SMF, Network Exposure Function (NEF), Network Resource Function (NRF), Network Slice Selection Function (NSSF), Policy Control Function (PCF), Unified Data Management (UDM), and Authentication Server Function (AUSF), among other 5G control plane functions, as required by the service provider. The operations, administration, and management are also deployed in the centralized 5GC data center. Apart from the SMF and AMF for the public- hosted MEC option, the rest of the control plane functions are deployed in the centralized 5GC data center.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 325, 'parent\_id': '863e43fb0aeca89f0044f45ed1c6a917', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '577116927193b5413978b180d95b612b', 'text': 'Now that we have an overview of the deployed network illustrated in Figure 5- 52, let’s look at some examples of multidomain threats and methods to mitigate the threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 325, 'parent\_id': '863e43fb0aeca89f0044f45ed1c6a917', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '57a1855e523165a3c1c4ff14d8b448bd', 'text': 'Threats: Case Study', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 325, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c14a0aa33455f226e14e313c835d2197', 'text': 'In this section, we will see some examples of threats that will impact multiple domains, such as edge compute deployed in the cloud, enterprise, and centralized data center. Out of all the multiple threat vectors illustrated in Figure 5-53, threat vector A and threat vector C are real-life use cases. Threat vectors A and C were not seen in a 5G environment, but the side-channel', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 325, 'parent\_id': '57a1855e523165a3c1c4ff14d8b448bd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '20001a5de7cb3531719d4d6f13c404ac', 'text': 'attack was seen in a service provider data center environment very similar to the one explained in this case study. Threat vectors B and D are added here to show the real scenarios you might face once 5G is deployed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 326, 'parent\_id': '57a1855e523165a3c1c4ff14d8b448bd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '1fa208cf2a2f5ac79c94bdaad398ac96', 'text': 'Broken Functional level Volumetric API attack DDoS attack Attacker CU, UPF, AMF , SMF o¥ - MEC applications (w P MEC hosted in Public Backhaul sniffing v cloud (for low latency o use cases) & Internet OAM, AMF , SMF, NEF, L Tk AP APT attacks o NRF, NSSF, a1 ""(A)) PCF, UDM, &= AUSF, UDM Centralized 5GC Public network / Containerized DU stored in a low footprint M2M devices DU, CU, UPF server in RAN site e MEC application £ \*4 Enterprise DC Enterprise MEC deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 326, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6dea901d41b28d6a14162439aa512c92', 'text': 'Figure 5-53 Example of Multiple Threat Vectors in the Deployed Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 326, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '434ca2edecbf2387ac62d90fd4751507', 'text': 'As shown in Figure 5-53, there are four key threat vectors we will look at in this section.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 326, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c037fb69ee3999021a255a8798e17f94', 'text': 'Threat Vector A', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 326, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3dcc4d2a9193af5f21e81f873ee8da2f', 'text': 'This threat vector is a DDoS attack caused by the attacker taking control of the unprotected IoT devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 326, 'parent\_id': 'c037fb69ee3999021a255a8798e17f94', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f3acd94b6c23d6b29eea5e39625bc724', 'text': 'Figure 5-54 depicts an attack based on volumetric DDoS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 326, 'parent\_id': 'c037fb69ee3999021a255a8798e17f94', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'b1d92ad8bf76106861ecd9f37aa7f921', 'text': 'Denial of service to legitimate users and high chances of server / software ¢ a crash leading to possible network outage and loss of revenue CU , UPF, Attacker ‘l e AMF , SMF \* S MEC applications MEC hosted in Public Multiple illegitimate cloud (for low latency requests [ use cases) & Internet : e e e s R | Multiple illegitimate i e St s e s requests m <+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 327, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '62aaccf61f0265ce67b7ced383d4cc04', 'text': 'Figure 5-54 Example of Attack based on Volumetric DDoS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 327, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '44880ca2fe2b1303cef0f24bfe47696c', 'text': 'As shown in Figure 5-54, the attacker exploits the unprotected IoT devices to cause an excessive number of illegitimate requests toward the MEC application database. This can overwhelm the MEC application database such that it cannot respond to legitimate requests, thus causing DoS to legitimate users. This can also lead to server or software crashes, leading to service outage and possible revenue impact.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 327, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'fb24acabe3b2a4ed242786432fdac062', 'text': 'Threat Vector B', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 327, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '16a0936ed681cd1a6e91eded34d7b6ac', 'text': 'This threat vector is called the Broken Functional Level API attack, which is based on a vulnerability in the API implemented by the developers or an unprotected API implementation by the service provider.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 327, 'parent\_id': 'fb24acabe3b2a4ed242786432fdac062', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1655886a8b7aacb3c4e0a3461e9c9f8b', 'text': 'Figure 5-55 shows an example of Broken Functional Level attack in an unprotected API.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 327, 'parent\_id': 'fb24acabe3b2a4ed242786432fdac062', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '3a56e80cbb180a33e2e10677d5fc57f5', 'text': 'MEC application a GET/api/users/myuserinfo MEC database v applications Legitimate User © GET/api/admin/alluserinfo » (hag @ Attacker Info of all users returned by MEC application database <', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 328, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '03080b98c68e4ee2495e3eb885564a0d', 'text': 'Figure 5-55 Example of Broken Functional Level Attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 328, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b52ae9c0f88b8b6755b0a467a8489e0', 'text': 'In the Broken Functional Level attack shown in Figure 5-55, the developer has used a generic implementation of the API, with the API relying on the client to use user-level or admin-level APIs. The threat vector is possible as the attacker figures out the “hidden” admin API methods and then uses them. As shown in Figure 5-55, the user is allowed to query their own user information from the MEC database. But due to the unprotected implementation, the attacker is now able to invoke some commands that are available to only privileged users. Now the attacker uses the admin privileges and exploits them to export the sensitive data, as seen in this example.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 328, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '97e1c9bed9e831f66b841ddfd128d18e', 'text': 'Threat Vector C', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 328, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ecc3526ec5e0b85d7220e94ea35e0180', 'text': 'This threat vector is based on advanced penetration threat (APT) attacks. The main aim of APT attacks is to gain information on the victim or targeted host illegally. The gathered information can be used to launch a large-scale attack on the target organization or to insert malware to encrypt all the sensitive files and destroy the goodwill of the organization by exposing the sensitive files on the Internet.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 328, 'parent\_id': '97e1c9bed9e831f66b841ddfd128d18e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ae03cc788f602af3866aafe7eb45f73f', 'text': 'Figure 5-56 shows one of the methods of an APT-based attack.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 328, 'parent\_id': '97e1c9bed9e831f66b841ddfd128d18e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '414ba01e3ba03d17527e53fe15fa7b69', 'text': "Victim Organizations data stored [ l—+ a in the attacker's storage server @ Attacker Malicious code inserted in the update Malicious code commands the database to push the config files Update and and other sensitive data to a Patches malicious C&C server = MEC application Vendor ; Update with malicious code used to update ® : the MEC application v DU, CU, UPF MEC Application e Trae (<A) — =3 Enterprise DC M2M devices", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 329, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1c1b234ed01b1d9cc491e338e905f26e', 'text': 'Figure 5-56 Example of APT-Based Attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 329, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4cc4aba5b6f234f7841ab463fd829ed2', 'text': 'The steps of this attack shown in the Figure 5-56 are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 329, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4f56317e83ee24ac7e64a3742bae5f33', 'text': '1. The attacker infiltrates the MEC application vendor and inserts malicious code within the update files or patch files intended to be implemented by the MEC application. This method ensures that the file available in the legitimate vendor’s website for download is infected by the malicious code.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 329, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '25926618c6f9f5028142c2bbc3718cf9', 'text': '2. The MEC applications are notified about the available update and then download the install file from the MEC application vendor’s site. The MEC applications will now undergo the update process and get infected by the update file with the malicious code.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 329, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ad3189c874ae5f765a47692df7931e2f', 'text': '3. Based on the intent of the malicious code within the update file, the MEC applications will behave accordingly. In our example, the intent of the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 329, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f5d8be66139a45a06414f313a6896747', 'text': 'malicious code within the update file is to open an encrypted tunnel to an external C&C server and start exporting the sensitive files.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 330, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '87fecbab1aa8667a59e2f9bc15446d38', 'text': '4. All the sensitive filed exfiltrated from the victim’s organization are now stored in the storage or C&C server, which can be accessed by the attacker. The attacker can now use the sensitive information in a variety of ways. One of the methods is to extort money by providing proof to the victim organization about the stolen data. The other method is to gather information about the organization and then carry out a surgical but devastating attack that causes maximum impact.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 330, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8dee2122b8538f0eab88aa0e0fa8311f', 'text': 'Threat Vector D', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 330, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '32c36f25cbc0b2e055af5d3fcdf4fa35', 'text': 'This threat vector is based on attacks due to transport vulnerabilities when public networks are used.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 330, 'parent\_id': '8dee2122b8538f0eab88aa0e0fa8311f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '24494028fc4497218d4ebb379ecea17c', 'text': 'Figure 5-57 shows an example of back-haul sniffing.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 330, 'parent\_id': '8dee2122b8538f0eab88aa0e0fa8311f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '848b9b4841d613e04027e7b12418a652', 'text': '[ a Attacker Backhaul sniffing OAM, AMF SMF, NEF, NRF, NSSF, Public network PCF, UDM, = AUSF, UDM N2 N4 Centralized 5GC v N9 @ DU, CU, UPF — o — | MEC Application Koo ((A>) +“— \_\_ Enterprise DC M2M devices MEC deployed in Enterprise Infra', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 330, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5ce5c055ebcaf3228e64dd6ad2c1d9ad', 'text': 'Figure 5-57 Back-haul Sniffing Due to Untrusted Public Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 330, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b7d7d22d09f89db987b9ec7f62b08292', 'text': 'In the example illustrated in Figure 5-57, the transport from the Enterprise MEC toward the centralized 5GC data center is based on the public network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 330, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c5b185112fb6d13dae56a3a858088a1d', 'text': 'The information carried in this transport from the enterprise MEC to the centralized 5GC involves the N2, N4, and N9 interfaces:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 331, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '94e05875fd38a8acb4966e0d31fea205', 'text': '• N2: Interface between gNB and AMF', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 331, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ce8a9ea516c95fa2f24f8999025ed86c', 'text': '• N4: Interface between UPF and SMF', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 331, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '374ae4d63ff8dd40450b819ebed161ba', 'text': '• N9: Interface between UPFs (UPF from MEC and UPF in centralized 5GC)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 331, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6fb3ae0c82f412b39e368aa916bbf76e', 'text': 'The N2 and N4 interfaces need to be protected for integrity, confidentiality and replay when using insecure public networks. They do not have these built-in security layers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 331, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c8ea8191307dc309c630bf06a2447ef2', 'text': 'Mitigation Examples', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 331, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8eef57a544aff4f2a292b4e3dd61a87e', 'text': 'This section takes you through the mitigation steps to secure the MEC deployment from the threats shown in Figure 5-53. This section will be of particular interest to readers trying to understand the exact scope of the threats and what specific solutions could be used as a tactical method to mitigate the four threat vectors, as shown in Figure 5-53 earlier in the chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 331, 'parent\_id': 'c8ea8191307dc309c630bf06a2447ef2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8d0413a6671180b6cb7d13cf49c1d172', 'text': 'Applying DDOS Protection and Securing API: Threats Vectors A & B', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 331, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2b24ec88f2c581df465ae88961ef31cc', 'text': 'Figure 5-58 shows the implementation of an API gateway to secure the API as well as DDoS protection techniques to protect the MEC deployment. For this example, the requirement of the DDoS protection is shown only for the MEC applications hosted in the public cloud as a defense mechanism against the device-based volumetric attacks on the MEC applications. An API gateway/API firewall is recommended in both types of MEC deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 331, 'parent\_id': '8d0413a6671180b6cb7d13cf49c1d172', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '388baa7fd44cd5c73798639f889716e7', 'text': 'DDo§ attack mitigated by using APl Gateway or AP! firewall MEC hosted in Public cloud (for capabiliies along with DDoS CU, UPF, low latency use cases) & Inemet AMF, SMF MEC applications \\E API Gateway / e S API Firewall . x» lemesassessena DDoS protection API / / OAM, AMF , Secure AP mitigating various SMF, NEF, SREETE APIthreats due to better NRF, NSSF, Centralized 5GC PCF, UDM, functional and object level s authorization, rate limiting, strict AUSF, UDM access control etc \\‘ $ M2M devices DU, CU, UPF Enterprise MEC \* . ( ) &MECappIicalion [y, deployment xRS Enterprise DC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 332, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6947ae2e20a2100e944c437c58f5e93a', 'text': 'Figure 5-58 API Gateway/API Firewall Deployments in MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 332, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7d9a8cc66aa3fb14eae4e0cecfa19ea8', 'text': 'As shown in Figure 5-58, the API gateway can be used as one of method to mitigate the API attacks. In this example, the API gateway/API firewall is deployed at the MEC locations as well as the centralized 5GC to protect the APIs from API vulnerable threats. The API gateway should have the following capabilities to protect the 5G applications and network functions from API- based attacks. The rate limiting and throttling features in the API gateway will provide protection against excessive request attacks from the IoT devices in the network. They will also secure the MEC applications from attackers trying to exploit any API vulnerabilities, such as Broken Functional Level authentication and authorization checks. This is done by having strict authentication and authorization checks carried out by the API gateway/API firewall against the identity, authentication, and authorization solutions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 332, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'db0ae0a828ea53b6b87f39d8d1d21d05', 'text': 'Depending on the MEC deployment model, an option of on-premises, cloud, or hybrid DDoS protection could be used. The DDoS protection is recommended to be deployed at the MEC implemented in the public cloud to thwart the DDoS attacks from the devices being catered to by the network. As this mode of MEC deployment is primarily to support URLLC use cases, the latency impact should be kept to a minimum and provide near-real-time response to requests. The DDoS solution implemented for the public cloud–hosted MEC applications should have features for scanning the HTTP request, and checks should be carried out on TLS version, HTTP version, query string, and user agent, among others.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 333, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8eb2654fdc90917f18bc1800e669f5ca', 'text': 'Securing MEC Deployments Against APT Threats: Threat Vector C', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 333, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a2ddd18faadd4350a06eab9d19b7de0', 'text': 'The threat vector in this example is based on the attacker inserting malicious code in the software updates or patches. The software update and the patch are then installed by the network device or virtualized network function (container/virtual machine). The malicious code can have a variety of malicious actions. The action in this example is for extracting the sensitive data from the 5G MEC application hosted in the enterprise data center. Once the data is extracted, the attacker can analyze it for any sensitive data, such as PII and network information. The attacker can then use the gathered PII to exploit the user data and sell the details on the web. The other method could be for the attacker to use the gathered network information to understand the type of network devices and software being used by the MEC data center in the enterprise network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 333, 'parent\_id': '8eb2654fdc90917f18bc1800e669f5ca', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3019dbcef6eadaef467fd5125134a58b', 'text': 'This section explains some methods for mitigating this threat vector.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 333, 'parent\_id': '8eb2654fdc90917f18bc1800e669f5ca', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '095e53357c3248ab8176b8f00559a534', 'text': 'Figure 5-59 shows one of the methods using an anomaly detection system to mitigate the APT-based threat vector.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 333, 'parent\_id': '8eb2654fdc90917f18bc1800e669f5ca', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '79be672435f8f0194cbd5354d8183fb9', 'text': "Threat Intel ' 0 [ ) Global Threat Attacker C&C server Intelligence feed Malicious code inserted in the update Data exfiltration and Data hoarding 10 C&C server detected and Anomaly detection [ ——— solution blocked by monitoring solution Update and Patches [ ——. Correction action by Anomaly (etection system, such as, MEC application Vendor Network | specific source traffic blocked Telemetry, from exting the infrastructure \\ Monitoring solution integrated with anti-malware container & 0 - detects malicious behavior after update and stops cloud telemetry | ssseal further updates from the update source 4 T A —— \\d et S e SRR R S I 0U, U, UPF | REpRp- MEC Application amma. y ( ) i cscasl — B3 Enterprise DC M2M devices R M e URa e i Eaint ok e S S e e", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 334, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c64011a2f496ce177b0174b3c5833e57', 'text': 'Figure 5-59 Anomaly Detection System to Mitigate APT-Based Attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 334, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67aa7af1512fd458b75c6d53c0613ae9', 'text': 'As shown in Figure 5-59, the attacker inserts a malicious code in the software update or patch files in the original update package from the MEC application vendor. The MEC application then downloads the update file for installing the software update. This could also impact the network devices if the update is for a firmware update for the MEC data center server or switches. The following steps would explain the method used by the anomaly detection system to mitigate this APT threat vector:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 334, 'parent\_id': 'c64011a2f496ce177b0174b3c5833e57', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '48137f0f66cea416ca7ba460b9656ddd', 'text': '1. The anomaly detection system is basically an intelligent network visibility and monitoring solution with enhanced machine learning and artificial', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 334, 'parent\_id': 'c64011a2f496ce177b0174b3c5833e57', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '44f47e15f12b8e417cedafd47ec8accd', 'text': 'intelligence algorithms. The anomaly detection solution will collect network telemetry such as NetFlow, jFlow, sFlow, IPFIX, syslog, events, and so on from network devices such as switches, routers, virtual switches, and so on. It would also collect telemetry from virtual instances, such as containers, and for virtual machines by using hypervisor telemetry. Cloud telemetry such as VPC logs can also be collected to have end-to-end visibility. Features like VXLAN stripping and packet de-duplication are required to make the information gathering more efficient.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 335, 'parent\_id': 'c64011a2f496ce177b0174b3c5833e57', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3c7fc99ec1b65c8d82693a0a1f2a9f48', 'text': '2. Analyze the data gathered and find any anomalies in it. For this to happen, it’s important that the normal network behavior is known. The normal network behavior, also known as baseline network, is identified by gathering the network information for 3–4 weeks and just feeding it into the learning database. This database is used by the anomaly detection system to learn what is normal behavior of the network and uses this as the baseline. Any variation from this threshold used for baseline will be considered abnormal behavior, otherwise known as anomalous behavior of the network. The anomaly detection solution should also have a very robust threat intelligence feed for global threat awareness. Having global threat intelligence would allow the advantage of the threats seen in any part of the world to be blocked if seen in part of the network. Threat intelligence is used to inform the threat intel consumers such as service providers and enterprises what threat actors are active, what attack model they use, the attacker’s intentions and motivations, and which malware arsenal they deploy. Having this information fed into the intrusion detection and prevention systems would give the systems’ algorithms access to a wide array of data as active threats emerge, thus providing effective mitigation actions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 335, 'parent\_id': 'c64011a2f496ce177b0174b3c5833e57', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b6db589638dd6f82beca1d264f29dfb7', 'text': '3. The anomaly detection systems will also indicate any actions of compromise, such as data hoarding and data exfiltration. This would need robust machine learning algorithms that are trained using data from such specific and targeted attacks. Once the ports through which the data is being exfiltrated are detected by the anomaly system, it will create alerts and necessary actions such as blocking the internal traffic from being exfiltrated.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 335, 'parent\_id': 'c64011a2f496ce177b0174b3c5833e57', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a72f99dcabed808f74c772a7756ebdb9', 'text': '4. One of the key techniques used by the APT is to use the encrypted traffic to prevent detection by IPS deployed in network. So, when a new device is infected by the malicious code within the software update, the device would then initiate an encrypted connection to the next connected host using the existing ports, thereby attempting to infect the neighboring host without', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 335, 'parent\_id': 'c64011a2f496ce177b0174b3c5833e57', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e22ab963abde8f9b3971e755df59f7b', 'text': 'detection. Here is where we need an enhanced visibility layer and mechanisms of detecting any malicious traffic without decrypting the encrypted traffic. This is provided by some vendors in the market today and enables the service provider/enterprise to detect malware in encrypted traffic. Once the anomaly detection solution detects the new behavior from the network devices and network functions after the software update/patch update, corrective actions can be used to prevent any more solutions being updated. As an added measure to counteract the malware propagation, advanced anti-malware solutions should also be used. The chosen advanced anti-malware solution should inspect the memory, CPU, firmware, software OS, and the application layer to identify malicious scripts and behavior using methods such as sandboxing. Once the source of the malware is found, it is recommended to quarantine the hosts and take preventive actions, such as halting the specific action that caused the malware intrusion.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 336, 'parent\_id': 'c64011a2f496ce177b0174b3c5833e57', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '139a12ae2da9f2b0ee462f42a82d3395', 'text': 'Securing MEC Against Sniffing Attacks: Threat Vector D', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 336, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '882b0fe1f926a5357e2e0ffc424709f5', 'text': 'The MEC deployment within the enterprise in this example requires back haul toward the centralized 5GC data center of the service provider. This back haul is vulnerable to a back-haul sniffing threat vector, as explained in threat vector D.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 336, 'parent\_id': '139a12ae2da9f2b0ee462f42a82d3395', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f558f4e6dd66f4da90113931d1a94f16', 'text': 'Figure 5-60 shows one of the mechanisms to mitigate back-haul sniffing at the transport layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 336, 'parent\_id': '139a12ae2da9f2b0ee462f42a82d3395', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c338f950747cc015e9f9e56e2fe50078', 'text': '[ [ Attacker Backhaul sniffing threat vector is mitigated due to the transport encryption using IPsec OAM, AMF , IPsec SMF, NEF, NRF, NSSF, N2 Public network B8 PCF, UDM, N4 = AUSF, UDM N9 Centralized 5GC DU, CU, UPF cama. MEC Application Koo = ( A)) . = Enterprise DC M2M devices MEC deployed in Enterprise Infra', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 337, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cc9ed5c07de25051a89cb190fe508d2d', 'text': 'Figure 5-60 Mitigation of Back-haul Sniffing Attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 337, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b898308d8c658223cb2def63d70a7ee4', 'text': 'Figure 5-60 illustrates the security control between the enterprise MEC and the centralized 5GC by implementing IPsec using a security gateway (SecGW). In the enterprise MEC deployment in this example, the transport for the N2, N4, and N9 interfaces uses the back hauling on the public network, which is insecure. To prevent any eavesdropping in the back haul, IPsec is recommenced. IPsec is a collection of protocols for security defined by the IETF RFC 2401 and provides data authentication, integrity, and confidentiality.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 337, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6649fb7f4f8ac986fb62547c2fcf36b2', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 337, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cea2317401e32f6bd4c50fd4a8ae3bd6', 'text': 'As discussed in this chapter, an MEC implementation will enable you to deploy low-latency use cases. Based on your chosen deployment method, you can implement MEC in the public cloud, on premises, on the enterprise data center, or you can choose a hybrid implementation. The “Threat Surfaces in 5G MEC Deployments” section took you through the different threats in the MEC deployment, the mitigations of which were explained in the “Securing 5G MEC” section. The “Real Scenario Case Study: MEC Threats and Their', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 337, 'parent\_id': '6649fb7f4f8ac986fb62547c2fcf36b2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '20b99a75747f9d6ec1d4b9b31e294794', 'text': 'Mitigation” section took you through the multidomain threat examples and their mitigations.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 338, 'parent\_id': '6649fb7f4f8ac986fb62547c2fcf36b2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd0fe78ab1ecd1a7199d3a376a4c9c509', 'text': 'Figure 5-61 shows you the multilayered security controls to secure the MEC deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 338, 'parent\_id': '6649fb7f4f8ac986fb62547c2fcf36b2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '07ca116e13d97c46d45d16dbfa24d5e9', 'text': '= < MEC & Internet ( A)) ) il - gNB + %:r] MEC hosted on Centralized 5G (Public cloud hosted / On- Packet Core gNB site premise / Enterprise datacenter) Inbuilt HW & SW security layer , SZTP Enhanced Access Control layer Application protection & Policy enforcement Enhanced Visibility, Anomaly detection, Analytics & Monitoring AP security (API Gateway, API Firewall) Security Gateway, NGFW, Advanced Anti-Malware & DDoS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 338, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'aadb78eabb664780e17cb6ed92a5d4c8', 'text': 'Figure 5-61 Multilayered Security Controls to Secure the MEC Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 338, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fe50b23bb22667e68b18087871ceedd7', 'text': 'Figure 5-61 shows the key security controls required to secure the various modes of MEC deployment. It has to be noted that you can share the security controls for other parts of the infrastructure if your 5G network deployment has other parts of the 5G infrastructure such as 5G RAN and 5GC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 338, 'parent\_id': 'aadb78eabb664780e17cb6ed92a5d4c8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '274f71c4b335eb432326ae1caf5955ac', 'text': 'The security control layers to secure 5G MEC applications and deployments are summarized as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 338, 'parent\_id': 'aadb78eabb664780e17cb6ed92a5d4c8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c875f0f97eb52db6e53fa9068a341979', 'text': '• Built-in hardening (hardware and software layers): The built-in security capabilities, such as hardened hardware and software, including', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 338, 'parent\_id': 'aadb78eabb664780e17cb6ed92a5d4c8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e59308311b6c094cc7b2d38afc5a7625', 'text': 'supply chain security and secure provisioning of the network components. This layer is usually checked or verified by a handful of service providers and enterprise customers. It is very important that you ensure that the built-in hardening is part of the checklist you include while selecting the vendors of your choice. The list provided in the “Hardening Hardware and Software” section in this chapter is a good place to start.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 339, 'parent\_id': 'aadb78eabb664780e17cb6ed92a5d4c8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'edcd79b27767ae52107e90aa2dfd6323', 'text': '• Enhanced access control layer: Having application access control based on the Zero Trust principles is a good way to have the security controls to focus on users, assets, and resources. The aim is to protect the 5G MEC resources such as MEC applications, servers, and network devices, irrespective of the MEC location (cloud/on premises/enterprise). For the enterprise MEC use cases, you should ensure that the access requests from assets located in the enterprise-owned network infrastructure meet the same security requirements as access requests and communication from any other non-enterprise-owned network. Due to the cloud-native mode of deployment in 5G, the MEC virtual instances are dynamic in nature, and the appropriate security controls should also evolve to secure the access to these dynamic components.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 339, 'parent\_id': 'aadb78eabb664780e17cb6ed92a5d4c8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a64f3c616fdf93c65f26d141a12ba9b0', 'text': '• Application protection and policy enforcement:. To secure the MEC applications and provide application-level visibility and policy enforcement, it is important to use a solution that can provide visibility at the application layer, including user-to-application mapping, enabling you with the option of strict enforcement on the applications. The application protection and policy enforcement layer should also scan all images before they run and enforce policy checking to ensure that they are allowed to be executed in your environment. The application protection and policy enforcement layer should also provide venerability assessment and capabilities of any forensics capabilities to investigate any abnormal behavior of the user or application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 339, 'parent\_id': 'aadb78eabb664780e17cb6ed92a5d4c8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fe0234a6920af246e37ff250e55ec032', 'text': '• Enhanced visibility, anomaly detection, analytics, and monitoring: Decrypting the packets, analyzing them, and then encrypting the packets again increases latency in the MEC applications. This might be an issue for URLLC use cases, some of which have stringent latency requirement of sub-1ms. An alternative would be to use intelligent solutions to cater for such attacks by identifying anomalies in the cipher suites being chosen and the behavior of the client/server handshake. This can be done by analyzing the packet header data, and there are solutions available today', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 339, 'parent\_id': 'aadb78eabb664780e17cb6ed92a5d4c8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '25f72af8d829d28532a574d5ed509f18', 'text': 'that can detect the malware within encrypted data without the need for decryption. The analytics part of this solution must also use the threat intelligence feed and combine it with the analysis of the gathered information using ML and AI algorithms to proactively detect any change in behavior of the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 340, 'parent\_id': 'aadb78eabb664780e17cb6ed92a5d4c8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a4d60d121264c92b7f4d5e167b7fb2b', 'text': '• API security: In 5G, APIs will play a much larger role of supporting intelligent flow of communications between the 5G network functions and applications for use cases such as IoT, M2M, and others. Having a strong, secure API strategy such as conducting penetration testing and audits on the APIs and applications using APIs will ensure that your API is secured and that any security holes/gaps are understood. The gaps can then be filled by ensuring the right feature or capability is enabled within the relevant security control. An example is a high value of rate limiting, which may allow DDoS/DoS attacks to be possible. A corrective measure such as optimizing the rate-limiting threshold can be performed to minimize the attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 340, 'parent\_id': 'aadb78eabb664780e17cb6ed92a5d4c8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9302035d50abe2d2fbd4ed236d071f85', 'text': '• SecGW, NGFW, advanced anti-malware, and DDoS security layer: MEC deployments such as enterprise deployments to fulfil enterprise use cases would need proper segmentation and encryption of the data being transferred between the enterprise sites and the centralized 5GC. Segmentation of traffic should be provided by an application-aware next- generation firewall (NGFW), which can apply policies based on the defined policy as well as protocols being used by the application; this will ensure that any malicious application within the enterprise network is not migrated to the service provider network and that any malicious instance from within the service provider infrastructure is not impacting the enterprise network. The NGFW should also provide audit and compliancy reports. A security gateway (SecGW) should be used when the 5G traffic traverses any public network or any untrusted network. IPsec uses a SecGW to mitigate the possibility of eavesdropping and man-in-the- middle (MitM) attacks. 5G MEC should also be protected by advanced anti-malware to protect the MEC network from malicious code that makes its way to the internal network. DDoS protection is an important part of the security control to mitigate attacks from internal devices within the MEC infrastructure and any inbound attacks from the Internet.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 340, 'parent\_id': 'aadb78eabb664780e17cb6ed92a5d4c8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0ae6bff1be1251f9defb156b97ec5873', 'text': 'Acronym Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 340, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '0a26f66ef1b66cadbf2f7058495ec72c', 'text': 'Acronym Expansion 5GC 5G Core AEF API Exposure Function AMF Access and Mobility Management Function API Application programming interface AS Access Stratum AUSF Authentication Server Function C-RAN Cloud RAN or Centralized RAN or Central RAN Cc2C Command and Control CA Certificate Authority CAPIF Common API Framework CCF CAPIF Core Function CD Continuous Development Cl Continuous Integration CNF Cloud-native function CcpP Control plane CuU Centralized Unit CUPS Control Plane User Plane Separation DCT Docker Content Trust DDoS Distributed denial of service DoS Denial of service DU Distributed Unit EAP Extensible Authentication Protocol ESP Encapsulation Security Payload FH Front haul FIPS Federal Information Processing Standard HSM Hardware security module IPsec IP Security ISAKMP Internet Security Association and Key Management Protocol M2M Machine-to-machine', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Acronym</th><th>Expansion</th></tr></thead><tbody><tr><td>5GC</td><td>5G Core</td></tr><tr><td>AEF</td><td>API Exposure Function</td></tr><tr><td>AMF</td><td>Access and Mobility Management Function</td></tr><tr><td>API</td><td>Application programming interface</td></tr><tr><td>AS</td><td>Access Stratum</td></tr><tr><td>AUSF</td><td>Authentication Server Function</td></tr><tr><td>C-RAN</td><td>Cloud RAN or Centralized RAN or Central RAN</td></tr><tr><td>Cc2C</td><td>Command and Control</td></tr><tr><td>CA</td><td>Certificate Authority</td></tr><tr><td>CAPIF</td><td>Common API Framework</td></tr><tr><td>CCF</td><td>CAPIF Core Function</td></tr><tr><td>CD</td><td>Continuous Development</td></tr><tr><td>Cl</td><td>Continuous Integration</td></tr><tr><td>CNF</td><td>Cloud-native function</td></tr><tr><td>CcpP</td><td>Control plane</td></tr><tr><td>CU</td><td>Centralized Unit</td></tr><tr><td>CUPS</td><td>Control Plane User Plane Separation</td></tr><tr><td>DCT</td><td>Docker Content Trust</td></tr><tr><td>DDoS</td><td>Distributed denial of service</td></tr><tr><td>DoS</td><td>Denial of service</td></tr><tr><td>DU</td><td>Distributed Unit</td></tr><tr><td>EAP</td><td>Extensible Authentication Protocol</td></tr><tr><td>ESP</td><td>Encapsulation Security Payload</td></tr><tr><td>FH</td><td>Front haul</td></tr><tr><td>FIPS</td><td>Federal Information Processing Standard</td></tr><tr><td>HSM</td><td>Hardware security module</td></tr><tr><td>IPsec</td><td>IP Security</td></tr><tr><td>ISAKMP</td><td>Internet Security Association and Key Management Protocol</td></tr><tr><td>M2M</td><td>Machine-to-machine</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 341, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'b23823f43ead0c41d93d4c0e4f31a213', 'text': 'MAC Medium Access Control MEC Multi-access edge computing MitM Man in the middle mMTC Massive machine-type communication NAS Non[nd]Access Stratum NEF Network Exposure Function NR New Radio NRF Network Resource Function NSA Non-standalone NSSF Network Slice Selection Function 0-CU O-RAN Compliant Centralized Unit 0-DU O-RAN Compliant Distributed Unit O-RAN Open RAN O-RU O-RAN Compliant Radio Unit O0AM Operations Administration Management PCB Printed circuit board PCF Policy Control Function PFCP Packet Forwarding Control Protocol PGW-C Packet Data Network Gateway [nd] control plane PGW-U Packet Data Network Gateway [nd] user plane PKI Public key infrastructure', 'metadata': {'text\_as\_html': '<table><thead><tr><th>MAC</th><th>Medium Access Control</th></tr></thead><tbody><tr><td>MEC</td><td>Multi-access edge computing</td></tr><tr><td>MitM</td><td>Man in the middle</td></tr><tr><td>mMTC</td><td>Massive machine-type communication</td></tr><tr><td>NAS</td><td>Non[nd]Access Stratum</td></tr><tr><td>NEF</td><td>Network Exposure Function</td></tr><tr><td>NR</td><td>New Radio</td></tr><tr><td>NRF</td><td>Network Resource Function</td></tr><tr><td>NSA</td><td>Non-standalone</td></tr><tr><td>NSSF</td><td>Network Slice Selection Function</td></tr><tr><td>0-CU</td><td>O-RAN Compliant Centralized Unit</td></tr><tr><td>0-DU</td><td>O-RAN Compliant Distributed Unit</td></tr><tr><td>O-RAN</td><td>Open RAN</td></tr><tr><td>O-RU</td><td>O-RAN Compliant Radio Unit</td></tr><tr><td>O0AM</td><td>Operations Administration Management</td></tr><tr><td>PCB</td><td>Printed circuit board</td></tr><tr><td>PCF</td><td>Policy Control Function</td></tr><tr><td>PFCP</td><td>Packet Forwarding Control Protocol</td></tr><tr><td>PGW-C</td><td>Packet Data Network Gateway [nd] control plane</td></tr><tr><td>PGW-U</td><td>Packet Data Network Gateway [nd] user plane</td></tr><tr><td>PKI</td><td>Public key infrastructure</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 342, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '2e6038a1848ffcbc42eb446d7ad6f163', 'text': 'RAN Radio access network RAT Radio access technology RBAC Role-based access control RIC RAN Intelligent Controller SA Standalone SBA Services-Based Architecture SCTP Stream Control Transmission Protocol SDL Secure development lifecycle SDN Software-defined network SecGW Security gateway SEG Security gateway SGW-C Serving gateway [nd] control plane SGW-U Serving gateway [nd] user plane SMF Session Management Function SSL Secure Sockets Layer SuCI Subscription Concealed Identifier SUPI Subscription Permanent Identifier SZTP Secure Zero-Touch Provisioning TLS Transport Layer Security TPM Trusted Platform Module UDM Unified Data Management UE User equipment up User plane URLLC Ultra-reliable low-latency communication VRAN Virtual RAN YANS Zero-Touch Provisioning', 'metadata': {'text\_as\_html': '<table><thead><tr><th>RAN</th><th>Radio access network</th></tr></thead><tbody><tr><td>RAT</td><td>Radio access technology</td></tr><tr><td>RBAC</td><td>Role-based access control</td></tr><tr><td>RIC</td><td>RAN Intelligent Controller</td></tr><tr><td>SA</td><td>Standalone</td></tr><tr><td>SBA</td><td>Services-Based Architecture</td></tr><tr><td>SCTP</td><td>Stream Control Transmission Protocol</td></tr><tr><td>SDL</td><td>Secure development lifecycle</td></tr><tr><td>SDN</td><td>Software-defined network</td></tr><tr><td>SecGW</td><td>Security gateway</td></tr><tr><td>SEG</td><td>Security gateway</td></tr><tr><td>SGW-C</td><td>Serving gateway [nd] control plane</td></tr><tr><td>SGW-U</td><td>Serving gateway [nd] user plane</td></tr><tr><td>SMF</td><td>Session Management Function</td></tr><tr><td>SSL</td><td>Secure Sockets Layer</td></tr><tr><td>SuCI</td><td>Subscription Concealed Identifier</td></tr><tr><td>SUPI</td><td>Subscription Permanent Identifier</td></tr><tr><td>SZTP</td><td>Secure Zero-Touch Provisioning</td></tr><tr><td>TLS</td><td>Transport Layer Security</td></tr><tr><td>TPM</td><td>Trusted Platform Module</td></tr><tr><td>UDM</td><td>Unified Data Management</td></tr><tr><td>UE</td><td>User equipment</td></tr><tr><td>up</td><td>User plane</td></tr><tr><td>URLLC</td><td>Ultra-reliable low-latency communication</td></tr><tr><td>VRAN</td><td>Virtual RAN</td></tr><tr><td>TP</td><td>Zero-Touch Provisioning</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 343, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b28e79acbbe6cfd3e8683d37e63e0086', 'text': 'Radio access network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 343, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '166df50f9764969145ddadd926990e5f', 'text': 'RAN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 343, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d7a8dac80fb34cde0a3c8c0c8ee668e', 'text': '3GPP TS 33.501, “Security Architecture and Procedures for 5G system,” Release 16, v 16.5.0, December 2020.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c8b3c5ee444c3ca2f323b3c12b7285d2', 'text': 'Pramod Nair, “ Securing 5G and Evolving Architectures,” Cisco Knowledge Networks, Cisco Public, September 17, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2f8e9ca309df2bed8d466522faf2e2cc', 'text': 'Pramod Nair, “ Securing 5G and Evolving Architectures,” Cisco', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ac2411bad6cf73518423ab8c9ae3f358', 'text': 'Knowledge Networks, Cisco Public, September 17, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1659aca680175cc67f5060b01042ad59', 'text': 'Pramod Nair, “Why 5G is changing our approach to security?”, Cisco Public, June 10, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d937cfa050212e0b1450ad730d32330', 'text': 'Pramod Nair, “Securing 5G cloud native deployments.” Open5GCon, September 30, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f43c2ea92ca19215cd8c55dbf430fa22', 'text': 'Cisco Service Provider VNI Forecast 2019', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b5055663f9605e2d3c3108124206025d', 'text': 'CISCO CYBERSECURITY SERIES 2019', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36e5e51833ea743f7bf3cd4c4c31e85d', 'text': 'https://github.com/kubernetes/kube-state-metrics', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5c213457ea5efd98f4fc5a5b2175d75a', 'text': 'https://owasp.org/www-project-top-ten/', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '78f80ebb10243c7d328eb9e25bd94349', 'text': 'https://digital.nhs.uk/cyber-alerts', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f28eaf80ee0f2c8bf9e6064083e90fdf', 'text': 'https://blog.talosintelligence.com/2020/12/xanthe-docker-aware-', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '13c669b171f2f8f971e8a6d1ad7cf359', 'text': 'https://blog.talosintelligence.com/2020/12/xanthe-docker-aware- miner.html', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b0a30fc76cad3bf2d21c081f7b556430', 'text': 'https://docs.docker.com/engine/security/trust/', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 344, 'parent\_id': '4bf253dfd25009abb79830a4c28ff6f3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '361c6b28c09249f5dccde41cd2b163ed', 'text': 'Chapter 6. Securing Virtualized 5G Core Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 345, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '62c2b95870d8f5186617d1f0e6ead30d', 'text': 'After reading this chapter, you should have a better understanding of the following topics:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 345, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4ef3f3abdbccacfc06c23d1446ce8da0', 'text': '• Threats in virtualized 5G packet core deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 345, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '613c2645ec639ce1cf0ee2ba975ed5be', 'text': '• Securing virtualized 5G packet core deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 345, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '81c848f9f26cb8711db49524140f3665', 'text': '• Real scenario case study examples of virtualized 5G core threat surfaces and threat mitigation techniques', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 345, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '34b29d8175794b30d08560fd3aaad149', 'text': '5G introduces service-based architecture (SBA) for 5G Core (5GC), which is designed for cloud-native deployment. This chapter will take you through the threat surfaces in virtualized 5G packet core Cloud-Native Function (CNF) deployments and mechanisms to mitigate the threats. The same threats and mitigation techniques would apply to the virtualized RAN CNF deployments as well, but as 5GC SBA architecture based on cloud-native architecture is mandated for 5G deployments by 3GPP, the focus of this chapter is primarily aimed toward the 5GC use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 345, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4a48bc913c2b09baa4b4a09b9e4709ee', 'text': 'This chapter will be of particular interest to the following teams from enterprise and 5G service providers deploying 5GC, 5G vendors developing 5GC products, and cybersecurity vendors planning new product developments and new functionalities to secure the deployment of 5GC:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 345, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '18965e748e6b350f333e1ba0d196c0f9', 'text': '• Mobile infrastructure strategy teams of service provider deploying 5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 345, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1bd1b55736bf76e3b9ddb5159133e4d6', 'text': '• Security strategy teams within service provider planning on deploying 5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 345, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '691016580914e4883a1f61f7420cf2d5', 'text': '• Security strategy teams within enterprise verticals planning on deploying 5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 345, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36f25947e2f2d72765bf466cde9f07de', 'text': '• Cloud computing and data center teams involved with 5G strategy and deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 345, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '22bbfcd98a3fab13fe6887ec3b541f7c', 'text': '• Security architects and design teams looking at securing the mobile infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 345, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3dd81cd4fbc3239ca5e39347f9273c2e', 'text': '• Enterprise solution and security architects deploying 5GC on enterprise premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 346, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8a921fab80a801461a501c77fb0d345c', 'text': '• Enterprise solution architects and enterprise security architects working with enterprises integrated with service provider 5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 346, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'be2ff1f38f8b16ffeac4e107c1551127', 'text': '• Government departments looking at regulating security for service providers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 346, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aa26be56eed8d9036a2ccd8b83dbe64d', 'text': '• Cybersecurity vendor security architects looking to secure 5GC deployments for their customers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 346, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a02d15e8342ac8f53e6dc34c393ec95f', 'text': '• Cybersecurity vendor product managers looking to enhance security products to cater for 5GC security use cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 346, 'parent\_id': '361c6b28c09249f5dccde41cd2b163ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5d8a3261c606152ad6a507a0b1209bce', 'text': 'A Brief Evolution of Virtualization in Telecommunications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 346, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e967cd1829c341166ae817c40bf91a81', 'text': 'Virtualization has been around since the 1960s, thanks to IBM CP-40, which was used to logically split the system resources in mainframes between different applications. But virtualization was primarily limited to mainframes, which made proprietary monolith hardware the norm for non-mainframe deployments. This followed into the data center (DC) world, where you had proprietary hardware from multiple vendors performing specific functions. In the telecom world, there was vendor-specific hardware such as Base Transceiver Station (BTS), Base Station Controller (BSC), transcoders, Mobile Switching Center (MSC) for 2G, NodeB, Radio Network Controller (RNC), Serving GPRS Support Node (SGSN), GPRS Support Node (GGSN), Home Location Register (HLR) for 3G and eNodeB, Mobility Management Entity (MME), Serving Gateway (SGW), and Packet Data Network Gateway (PGW) for 4G. These were deployed in the telco data centers as monoliths.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 346, 'parent\_id': '5d8a3261c606152ad6a507a0b1209bce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6053ac2b851514f31fcdf4602e29f1c7', 'text': 'Then came the first stages of virtualization, where you had physical servers racked in your data center with an operating system deployed on top of them, and a specific application could now be deployed on top of this operating system.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 346, 'parent\_id': '5d8a3261c606152ad6a507a0b1209bce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9d49d8303ca50d9052e6aeba050047cc', 'text': 'Telco vendors saw this as an opportunity to deploy the network functions, but the service providers wanted a data center with a single operating system that could be used to deploy the network functions. This led to the evolution of the hypervisor, which existed since the 1960s. This required an evolution in the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 346, 'parent\_id': '5d8a3261c606152ad6a507a0b1209bce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b390b7e96a96fe029fc88d044bce5d30', 'text': 'hardware as well, and x86 server chipset vendors started to add hardware virtualization in their chips, which happened around 2005.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 347, 'parent\_id': '5d8a3261c606152ad6a507a0b1209bce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e4c1ba12101ef0a1dfc354da6cdcd2fa', 'text': 'You were able to reuse your data center servers, but rather than installing a single operating system and specific custom application on that server, you could install a hypervisor operating system and use it to deploy multiple virtual machines (VMs) that can run many different network functions all at the same time in a single x86 server. This gave you the advantage of optimizing your data center resources for telco deployments and the flexibility to deploy the network functions wherever you had a data center footprint.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 347, 'parent\_id': '5d8a3261c606152ad6a507a0b1209bce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a71dcf66007924b30047d31d3294f185', 'text': 'Then came more innovations in the computing world in form of containers and cloud-native deployment models. The cloud-native approach is a method of building and deploying applications enabling you to fully consume the advantages provided by cloud deployments. You can fulfill the cloud-native approach using both virtual machines (VMs) or containers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 347, 'parent\_id': '5d8a3261c606152ad6a507a0b1209bce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3a17bd05e1b45d3a3d905c93986edeb6', 'text': 'Containers are very lightweight and provide a standalone executable software package that is self-sufficient and includes everything to run on, including executables, binary code, libraries, system tools, and so on. These containers will always run the same, regardless of the infrastructure where you plan to deploy them. This allows you to create a network function in any program of your choice, deploy it in any infrastructure of your choice, use any hypervisor of your choice, deploy it on any public cloud infrastructure, and also deploy it on bare metal. The telecom industry saw this as the right opportunity to use a new cellular technology to take advantage of these innovations.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 347, 'parent\_id': '5d8a3261c606152ad6a507a0b1209bce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3a33c0e87ef159de7897a0ceffc96aca', 'text': 'Enter 5G. 5G is the first technology to make use of open source and Cloud- Native Functions to deploy network functions. The key idea is to make it extremely flexible to deploy so that you don’t have to worry about proprietary hardware, software stacks, or interfaces for interoperability. You just need to think about creating new use cases and business models. When we look at the container deployments today, the most widely used container platform is Docker, and Kubernetes is the most widely used orchestration layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 347, 'parent\_id': '5d8a3261c606152ad6a507a0b1209bce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'baaee1885af2ed381209654919f97a00', 'text': 'Figure 6-1 illustrates the evolution in telecom infrastructure from physical monolith equipment in 2G and 3G to the virtualized cloud-native deployments in 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 347, 'parent\_id': '5d8a3261c606152ad6a507a0b1209bce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '71927612d42be2fd821925cd4b370e55', 'text': '2G, 3G, 4G 4G 5G Physical servers Virtual machines Containers/ Kubernetes/ (months to deploy) (deploy in mins) Microservice (deploy in secs) Vitual Virtual Virtual Containerized Applications Machine Machine Machne g : il Hyperviso BTS, BSC, MSC, RNC, SGEN... Increasing compute Reducing Increasing attack flexibility costs surface —', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 348, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '75c6462918d58afd8b9dbc5ec49f07da', 'text': 'Figure 6-1 Evolution of Telecom Infrastructure from Monolithic to Cloud Native', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 348, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5bfc088249d61c0be9c0f47c6c7af870', 'text': 'Native', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 348, 'parent\_id': '75c6462918d58afd8b9dbc5ec49f07da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '22f2c965d2f9ea15c790aaf458d296a8', 'text': 'As shown in Figure 6-1, while virtualized cloud-native deployment of 5G network functions such as 5GC and 5G RAN allows flexibility and scalability, it brings in new vulnerabilities. Although the system resource utilization in proprietary physical servers used in legacy cellular technologies like 2G and 3G is poor, it allows good isolation by providing physical separation of management and the user plane, including options of separate ports, line cards, and CPUs. Deployment of 4G network functions using virtual machines allowed multiple workloads to be deployed on a single x86 server. This provided a more efficient use of system resources and also provided isolation by permitting applications to run in a guest operating system. As compared to the proprietary monolith hardware, VM deployments offer less isolation because the same CPUs and interfaces can be used for control plane and user plane. When VMs are being installed, you have to allocate RAM and CPU resources that are earmarked for the VM instance regardless of whether usage leads to wasting resources. The VMs copy not only the operating system instances but also the libraries, binaries, and copies of the virtual hardware needed by the OS. Repetitive files suck up a large part of the RAM and CPU resources of the servers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 348, 'parent\_id': '75c6462918d58afd8b9dbc5ec49f07da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b16b942eaab56db47bdc97010de87fa7', 'text': '5G Cloud-Native Functions (CNFs) deployed using containers or VMs provide a very flexible deployment model because they are lightweight and it’s easy to deploy within an on-premises data center or public cloud. Container deployment in 5GC provides effective resource usage, as the container is packaged with dependencies from the operating system, binary code, libraries, and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 349, 'parent\_id': '75c6462918d58afd8b9dbc5ec49f07da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0ae8bbe819cacd9ebf5ab5da1e89fc76', 'text': 'Although virtualization provides better resource optimization, flexibility in deployment, and reduced cost, the attack surface has also increased due to the dissolving perimeter. This is because 5G RAN and 5G Core (5GC) CNFs can now be deployed in any public cloud provider’s infrastructure and on-premises DC along with other existing applications, and the 5GC NFs can be developed using open source software stack that might have existing vulnerabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 349, 'parent\_id': '75c6462918d58afd8b9dbc5ec49f07da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6d43f5943c966953d199a841ea8d9482', 'text': 'Figure 6-2 illustrates the key 5GC control plane and user plane CNFs, further defined in the list that follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 349, 'parent\_id': '75c6462918d58afd8b9dbc5ec49f07da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '1a6029cb28055589cc8973e9f1d9a924', 'text': 'NF Primarily deployed on: A Central DC (Network Functions) ¢ Public Cloud 5G Packet Core CNFs - Key Control Plane Functions = i //\\ ,,,,,,,,, ToMEC UDM PCF AF NEF | < » applications / = NRF | T other NFs Nudm Nnssf Nnrf Npcf Naf Nnef‘ I@{ i To Nausf Nsmf Namf Roaming H SCP | AUSIF |\_ AVF \\ partners e e . D e e S S e D ey | SBI (Services Based Interface) / Primarily deployed on: \* Edge DC (Services Based Architecture)l \* Public Cloud 5G Packet Core CNFs - User Plane [[—1 (. | | UPF', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 349, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9bd29e42585fe596f857ece9994809bb', 'text': 'Figure 6-2 Key 5G Control Plane and User Plane Network Functions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 349, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '080257c2a71d3bd03a37d392b8115b33', 'text': '• Network function (NF): 5GC is composed of cloud-native, virtualized functions to support a wide array of use cases. 5GC CNFs are basically 3GPP 5GC control plane and user plane functions that are deployed to fulfill the 5G use cases. The control plane messages are mainly between the 5GC NFs. The user plane messages are mainly between the user equipment and Internet, with the User Plane Function (UPF) providing the interconnect, encapsulation, and decapsulation of GPRS Tunneling Protocol User Plane (GTP-U) and other functions related to the user plane traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 350, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ba3f68acf085f99605c3e6889af09b7f', 'text': '• Service-based architecture (SBA): SBA is a framework for 5GC CP communications with the aim of replacing signaling messages by API calls. It also replaces the point-to-point signaling used in legacy technologies such as 2G, 3G, and 4G with a service bus everyone-to- everyone communication. As illustrated in Figure 6-2, the principles of SBA apply only to the control plane functions of the 5GC. Using the SBA framework, you have the option of using any vendor for any network function. For example, you could have AMF/SMF from Vendor A and NSSF/AUSF from Vendor B. As SBA uses API calls for communications, you shouldn’t really have any issues with interoperability. Having the SBA framework, you can now also deploy the network functions in the public cloud. Another advantage of SBA is that it enables developers to develop applications that interact with the 5GC components using API calls using Network Exposure Functions (NEF).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 350, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '23f4255f5e3164544cc81304c40a79bc', 'text': '• Service-based interface (SBI): SBI is the term used for the API calls between the 5GC network functions in the SBA architecture. The design principles and documentation guidelines for 5GC SBI APIs are specified in ETSI TS 29.501. All 3GPP NFs has a mandatory requirement to support TLS, which should be used if other means of network security, such as Network Domain Security (NDS) using security gateways (SecGW/SEG), are not implemented in the 5GC PLMN network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 350, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b1e4feba86a9f56050034d0a4e583485', 'text': 'Figure 6-3 provides the view of the deployment locations for the 5G cloud- native control plane and user plane components.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 350, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '0d8fa016f499f1970ffea4411bde87d8', 'text': '5GC Control Plane CNFs 5GC User Plane CNFs m = [« — ] =] = = @ On-prem Radio MEC - Central DC . Node location On-prem DC or Public Cloud On-prem DC or Public Cloud', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 351, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8cfb53755b565445754ae2aece88c75c', 'text': 'Figure 6-3 Deployment Location Options for 5GC Control Plane and User Plane Network Functions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 351, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '73233a97339f78da46b5bd8bc121cf88', 'text': 'As shown in Figure 6-3, the 5GC user plane (UP) components can be deployed even at the radio node location to enable ultra-reliable low-latency communication (URLLC) use cases. The 5GC control plane (CP) functions can also be deployed in the radio node location, but because the latency requirement is specifically for user plane and because the server at the radio node has an extremely low footprint, there is no need to have the 5GC CP functions deployed at that location.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 351, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0424f0708a94b3b3983c3b219962be1c', 'text': 'Although the 5GC CP CNFs can be deployed in the edge and central DCs, most of the use cases today do not need the CP to be deployed at the edge.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 351, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da45d9e0b67a46b5bfc91b73e7bc749c', 'text': 'Figure 6-4 illustrates the different modes of 5GC NF deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 351, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5cf763d37b7eaed3ce67bbeb65ae535e', 'text': 'Containers Virtual Machine g A /\\ 4 AMF | | SMF UPF SMF| |NRF UPF 5 B Container AMF | | SMF N R F || UPF S 0 Q Runtime Ea Cont: alr ner Runt ime Host OS % . Infrastructure ill E . Infrastructure | S 5G CNF as VM 5G CNF as Containers on VM 5G CNF as Containers on BM', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 352, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '76f31103f5a7aa82281028f95d233c21', 'text': '5G CNF as VM', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 352, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '359ef229b442a54335a6d6c096b2c6b6', 'text': '5G CNF as Containers on VM', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 352, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a85f18f8cc7dd7589abc322da03913f5', 'text': '5G CNF as Containers on BM', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 352, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ecc64469448374aaf7f667ecf36b9796', 'text': 'Figure 6-4 Deployment Modes for Cloud Native 5G Packet Core Functions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 352, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '47ce5acf5fa2b955db9e6b39fe3442d7', 'text': 'Service providers and enterprise verticals want a choice of deployment models to enable use cases. The reasons could include whether you want to support multiple modes of deployment based on use case and workload type or to accommodate an existing single-cloud deployment or due to a shortage of resources for optimal deployment of a specific method. You want the flexibility to be able to run containerized applications on bare metal (BM) or virtual machines (VMs) in your on-premises data centers, whether on a RAN node location, an MEC or centralized DC, a multistack public cloud, or a hybrid deployment model. As shown in the Figure 6-4, there are three options for deploying 5GC CNFs that can be deployed on premises or in the multicloud public cloud stack. One option is based on a virtual machine and the other two options are based on containers:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 352, 'parent\_id': 'ecc64469448374aaf7f667ecf36b9796', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3b4d40ff548f3df56e7d14e30be454c7', 'text': '• 5GC CNF as VM: VM deployment is not a new deployment model. Many of the test beds used initially for 5G non-standalone model (NSA) used the virtual network functions of 4G and upgraded the software to provide initial 5G NSA services. Many vendors also have parts of their 5GC network functions in VM format to make full use of the service provider’s resources. All the major vendors are moving toward the container in VM and container in BM models to make full use of the cloud-native approach.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 352, 'parent\_id': 'ecc64469448374aaf7f667ecf36b9796', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8c4cfeb4f1a04b65983fa19a7088677c', 'text': '• 5GC CNF as containers on virtual machine (VM): Having 5GC NFs deployed as a container on VMs is the option many service providers are choosing to deploy, mainly because of infrastructure readiness and lack of readiness from 5GC vendors in providing a true container stack. Many of the service providers are also heavily invested in a single private cloud platform, and a step in the direction of deploying containers on VMs is in the right direction of moving toward the hybrid cloud environment. Deploying containers on VMs will provide you with better isolation as compared to deploying containers on bare metal. Containers deployed on VMs are also easier to move between hosts using guest images.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 353, 'parent\_id': 'ecc64469448374aaf7f667ecf36b9796', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8a86165f11755e7d5783857f64beff8e', 'text': '• 5GC CNF as containers on bare metal (BM): Containers being deployed on bare metal will actually provide you with better performance for 5GC use cases. Containers deployed on bare metal utilize system resources better than containers deployed on VMs. One of the key reasons is the direct access to physical hardware. This makes it suitable for low- footprint server deployments, such as in the gNB locations, with a customized CPU for better performance in MEC use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 353, 'parent\_id': 'ecc64469448374aaf7f667ecf36b9796', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4cd21cb44bcd555aa159edc0d448afb3', 'text': 'Threats in Virtualized 5G Packet Core Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 353, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '19203f7f26865ab4c2b1695901c3ecde', 'text': 'As deployment methods have moved from hardware monolith models to virtualized cloud-native models, the attack surface has also increased. Using the CNF approach for building 5GC NF components means that an open source software stack is used to develop the 5GC NFs, which increases the risk in 5GC deployments. This section is dedicated to explaining the different threat surfaces in a virtualized 5GC CNF deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 353, 'parent\_id': '4cd21cb44bcd555aa159edc0d448afb3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'de88c2379768728d10048dd4899435ea', 'text': 'Figure 6-5 illustrates the threat surfaces for different 5G RAN and core CNF deployments. This section will take you through the 5GC container, internal, and external 5GC NF vulnerabilities. The hardware vulnerabilities are covered in Chapter 5, “Securing MEC Deployments in 5G” in the section “5G MEC Infrastructure and Transport Vulnerabilities.”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 353, 'parent\_id': '4cd21cb44bcd555aa159edc0d448afb3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '2481ecd0017594bc994a5212539dfe68', 'text': '5G CNFs deployed on mix of 5G CNFs deployed only on 5G CNFs deployed only on Public Private Cloud, programmable Cloud providers (GCP, AWS, Azure on-premises & multi-stack routers, low footprint servers, etc) & Public Cloud provided by 5G Public Cloud MEC Equipment Vendors Public Cloud O provider L] Container AP | 5G 3" party vulnerabilities vulnerabilities Public Cloud provider p Applications Container API wvulnerabilities 4 uinerabilties PO S— JR—— eI CEERr) Y H ¥ e ] a&ﬂj“ % m T 5GC UP NFs é ’SGC ;F’P NF S 5G 39party é\\ 5G RAN & 5GC UP NFs E 4 | 5GCCPNFs ‘\\é | Applications - \_\_\_\_\_\_ o /w | Container AP Hardware & — = Host = NFVI NFVI vulnerabilities vulnerabilities vulnerabilities NFVI Hardware & Host vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 354, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f74ea9133db526409df428b6bc34e049', 'text': 'Figure 6-5 Threat Surfaces for 5G CNF Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 354, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9a55340de88f5e3648f0e85897e4bd72', 'text': 'Figure 6-5 shows the two models of deploying the 3GPP 5GC network functions: on the public cloud and the on-premises data center. These new deployment models require a good understanding of the multiple cloud-native component integrations and the different layers of testing required to achieve secure cloud-native deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 354, 'parent\_id': 'f74ea9133db526409df428b6bc34e049', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '345d09ea9778319dc8ea85adbb09e058', 'text': 'The threats within the 5GC container deployments can be broadly split into three categories:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 354, 'parent\_id': 'f74ea9133db526409df428b6bc34e049', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'text': '• 5GC container vulnerabilities:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 354, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b6fd7dbc72e2da5205b6e1f492dfcbb1', 'text': '• Insecure container build', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 354, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6e53dab71ceb5820786106b0d9d7e708', 'text': '• Image vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 354, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ab3a68e95f2be8c6498d67a9cc07e4ac', 'text': '• Container runtime vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 354, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5adb5f9f6823e1763e93c1f7e589bcad', 'text': '• Insecure container host', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 354, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '033becd7ca29014e0cfd98e28e2b381e', 'text': '• Malicious container network traffic', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 354, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eb4da38b0300b4b4186ffafb2036bdce', 'text': '• Malicious 5GC CNFs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 354, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd5ccd778b726c0094cfb21e9992d2201', 'text': '• Insecure container management and orchestration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 354, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9864f6af937ada8cb222f021b9e08aed', 'text': '• Improper access control', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '46adc214cb7b24bea6a08671df509481', 'text': '• Improper configuration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '436f2e7b328579430d61d7e3f7ccb034', 'text': '• Insufficient isolation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '26ac352e91b2855c0f2a1a454f3b085d', 'text': '• Insecure container networking: This can be split into two areas— internal container communication within a pod and communication with external pods or servers:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2464295ab3da0b188b6779542c282b8f', 'text': '• Internal interfaces:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '497f9e380a5e25ff735ffe071af2a64f', 'text': '• API vulnerabilities within SBI communication', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dd42631690415e29b713323117589c39', 'text': '• Insecure network leading to eavesdropping', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '08c1cdd94704f9c5d2c3fb97a432d671', 'text': '• External interfaces:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1929aabb3c0c35faa7a8bd9523941f32', 'text': '• Improper isolation and segmentation with enterprise network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '599fe4497d658131fe55aa156474031f', 'text': '• API vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd4ae1d668e5101eb84b22224a4f8488b', 'text': '• Vulnerabilities relates to non-3GPP MEC NFs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7f75d9a6628a77739985f61af0f17c10', 'text': '• Insecure roaming interface and misconfigurations', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6af9e50115d9c7b77ade70f29f61c5b8', 'text': '• Hardware and host OS vulnerabilities:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '55576acf199ab04a7ad7220deb331624', 'text': '• NFVi hardware and software vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6dd9edae4919e2472c5994d01d67a637', 'text': '• Improper access control', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '723e68f4e4f8e7ae84debc1a7e51d361', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '41cd8688ce6cd03a239b073311782f9e', 'text': '5GC Container Vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a34a36588903bdb0d92f6f7f7ea23438', 'text': 'In previous cellular technologies, there was very little to no deployment related to container technologies. Use of container technology for 5GC NFs necessitates the Continuous Integration/Continuous Development (CI/CD) process, which helps you achieve quicker delivery of applications. If you are a 5GC vendor, you will use the CI/CD process to build your 3GPP 5GC NFs. If you are an enterprise or service provider, you will use the CI/CD process to build non-3GPP 5GC NFs to interact with 3GPP 5GC NFs for various use cases such as enhancing the functionalities of the 5GC NFs or allowing integration for enterprise use cases and monetizing 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '41cd8688ce6cd03a239b073311782f9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '55630e98ec4fa5c5c8a54e430b0cbb82', 'text': 'Simply following the CI/CD process is not enough to build the 5GC NFs. CI/CD, while ensuring quicker development of application, also brings in new threat surfaces related to insecure 5GC NF images and their distribution. 5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 355, 'parent\_id': '41cd8688ce6cd03a239b073311782f9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd3df84bd44a7539dd95b856036e359cf', 'text': '3GPP and non-3GPP NFs are susceptible to vulnerabilities and malicious software, which pose a threat during runtime. The malicious images could be used by an attacker to exfiltrate sensitive information or cause DoS attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 356, 'parent\_id': '41cd8688ce6cd03a239b073311782f9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5f92a3e6b3a66689c4bba6180dd0ed67', 'text': 'Figure 6-6 illustrates the key threat surfaces in the container runtime environment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 356, 'parent\_id': '41cd8688ce6cd03a239b073311782f9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5ed85075b705deaa5b403388b2b12b4f', 'text': 'Attacker scans and identiies Attacker aware of the vulnerability unprotected container images Attacker exploits the vulnerability of the program in container images - W——— == z Developer 0 5GC NF deployed in 3 Developer uses software components with gmmmem— /V public cloud e W T 0 - unpatched vulnerabilties Data Exfilration to create 5GC container g — i E 5GC NF i image build Unprotected container images in container repository 5GC NF deployed on-premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 356, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4a8926605bf471debca71f1fb9df9dc4', 'text': 'Figure 6-6 Key Threat Surfaces in Containerized Runtime Environment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 356, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ea29392c27c0fc3186a588942c5955dd', 'text': 'The text that follows describes the threat surfaces illustrated in Figure 6-6.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 356, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '877c6b05a396b5ed233a3cfaa82731bc', 'text': '5G provides the flexibility to build or create 5GC network functions with open source components to make them truly deployable in a cloud-native environment. Cloud native, a term used to describe container-based deployment, is a new concept in 5GC deployments. The network abstraction brought along by 5G addresses not only the need for portability across cloud environments but also the ability for developers to take advantage of emerging patterns to build and deploy applications. Some of the key threat surfaces illustrated in the Figure 6-6 are as follows.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 356, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1f30b867c101c36e2010bd221540eca2', 'text': '1. The developer for the 5GC vendor uses open source software to build the 5GC network functions. One of the threat surfaces here is the existing vulnerability of the program being used to build the image.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 357, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8f76614db8c3e1683062706fdefaf636', 'text': '2. In example shown in Figure 6-6, the developer uses software components with an unpatched vulnerability, images missing critical security updates, or outdated patches. Once the developer builds the image with an existing vulnerability in the software components, it leads to the image having built- in vulnerabilities that can be exploited by attackers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 357, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3b214f7764ad9e134eb735db27927207', 'text': '3. Once the image is built, it is stored in a container repository. You will then download the containers from the container repository and deploy them in your network. If you download an image that has an embedded vulnerability, it might make your network vulnerable to attacks due to attackers exploiting the known vulnerability.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 357, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c39435adbfb6baa09f1204d1b8ee319e', 'text': '4. Another attack vector at the container repository is the attackers scanning the images in the container repositories for any unprotected containers and then exploiting them. This attack vector is explained in detail in the section “Virtualization Threat Vectors” in Chapter 5.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 357, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8f2cea7aff517c76df0c436649345128', 'text': '5. Once the vulnerability in the deployed 5GC network function is exploited, the attacker might be able to map other systems in the environment, attempt to elevate privileges within the compromised container, or abuse the container for use in attacks on other systems.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 357, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '157096063deba9390bb4399359e7eff7', 'text': '6. Due to the portability and the modular characteristics of containers, the packages can be configured once and deployed on multiple servers or multiple cloud instances. An example would be a user plane component like User Plane Function (UPF) or a control plane component like Session Management Function (SMF), which can be deployed in multiple edge on- premises servers or public cloud with a predefined template. If the attacker exploits the UPF image within the container repository, all the UPFs deployed within your infrastructure are now susceptible to attacks such as exfiltration to a command and control (C&C) server defined by the attacker in the exploited image.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 357, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '61c29c3163128f973fd3c44b542eb206', 'text': 'Apart from the aforementioned vulnerabilities in the container build and runtime, other key container vulnerabilities are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 357, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e7ccc071df94e8e58305b0516059ca4d', 'text': '• The container registry is a location where you will store and distribute images. The registry will be used by vendors to upload signed images that you can download and deploy in your network. The registry will also be', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 357, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0fe7a6031d003f229e1aa2d9d237efa0', 'text': 'used by you if you are developing an 5GC application and would like it to be deployed across different parts of the network. Due to the container environment where an application can have tens or hundreds of containers, depending on the use cases, you might have thousands or tens of thousands of containers in the registry. An insecure container registry or API implementation of the containers can lead to attackers having access to the containers, and the attackers can exploit any weakness to deploy malicious code within the container that you have uploaded to the registry or replace the container with a malicious version.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 358, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dddcb6d287ec4443e6bf9818cd9c6ccf', 'text': '• Patch management is another area that is impacted by the deployment of container-based network functions. In existing technologies where the deployments are based on proprietary hardware or virtual machine instances, the patches are usually provided by the vendors a couple of times per year. The real issue for you in relation to 5GC containerized network function deployment is the time taken to patch the vulnerability in the open source component of the 5GC CNF. An example would be one or two major patches coupled with one or two maintenance patches per year. Container deployment is basically deployment of disaggregated software, and this will allow increased updates, basically destroying the existing 5GC container and deploying a new image with the updated patch. There are a couple of risks attached to this new procedure. One of them is having gaps in visibility and monitoring in understanding which of the deployed 5GC network functions are up to date. The other key risk is an improper patch update procedure ensuring right configurations and security policies are applied to the latest 5GC container image. Normally when a vulnerability is disclosed in open source software, the person who finds the vulnerability reports it through the open source community. The 5GC vendor should now create a customized kernel with the patch and follow the procedures for signing and uploading it to the registry. This should then be downloaded, the old container image destroyed, and new the container image with the vulnerability patched should be deployed. The key issue here is the time taken between the vulnerability disclosure and deployment of the new container in your 5GC environment. This gives enough time for an attacker to exploit the vulnerability and cause harm to your network or exfiltrate critical information. One other key issue is the customization of the Linux kernel used in a 5GC containerized deployment. This will further extend the time taken to provide the patched container image, as you cannot just patch it from the upstream kernel. In', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 358, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4af7f27133678deaf1cf0e915b2db3b0', 'text': 'short, patch management for the 5GC components should be one of the key criteria that’s thoroughly discussed with the 5GC vendor.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 359, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '34e50b2f6db54ab69880c75d6db14140', 'text': '• The very dynamic nature of 5GC container-based network functions during runtime can make it very difficult to monitor them. The key risk here is the lack of visibility in the dynamic container environment to detect any anomalies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 359, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2b2e1ea784a0ea7e835911d00c709daa', 'text': '• Improper configuration of a 5GC container-based network function such as the 5GC components running with a higher privilege is another area that can lead to your network being compromised.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 359, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a45827e50d105d0bdf0d3e276cca971', 'text': '• One of the reasons for the increase in threat surfaces in virtualized 5GC NFs is due to the polyglot nature of microservices, which is the result of the flexibility in using multiple open source components in 5GC. This threat surface is explained in Chapter 5 in the section “Virtualization Threat Vectors.”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 359, 'parent\_id': '4a8926605bf471debca71f1fb9df9dc4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8475aa055f448c54243a0b2d141d3f99', 'text': 'Insecure Container Networking', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 359, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9b32d5d10b6c88f39ae44fa5ca955756', 'text': 'In 5GC container-based network function deployments, the communications are based on the service-based interface (SBI), which employs REST interfaces using HTTP/2.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 359, 'parent\_id': '8475aa055f448c54243a0b2d141d3f99', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e441cf87046e7a607841fbf6796788d8', 'text': 'As illustrated in Figure 6-7, there are multiple interfaces in 5GC where the REST API calls would be used, such as the SBI message bus for control plane communications within the 5GC network functions, by the Network Exposure Function (NEF), which exposes capabilities and events to third-party Application Functions (AFs) and the orchestration layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 359, 'parent\_id': '8475aa055f448c54243a0b2d141d3f99', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f4f15c69f2883b5e98e08f7882a0c5c8', 'text': 'i API iAPI R N N N A N AT SBI Message Bus (API) SBI Message Bus (API) AP ubm AMF | oswF | sepp | 1 : S —— | ; S — \\: (On-premises or (On-premises or = ") cloud Infrastructure) &b cloud Infrastructure)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 360, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0041aab5296fff40465675df630925ed', 'text': 'Figure 6-7 API Communication in the 5GC Environment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 360, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0c8e371e48a494052c1802e3f717555d', 'text': 'The deployment of 5GC containers also requires orchestration for creating, operating, and managing the containers. One of the most popular container orchestration tools used today is Kubernetes. While deploying 5GC CNFs, the majority of the service providers and enterprise verticals plan to use Kubernetes as an orchestration tool. One of the main reasons for this is the existing skillset within the in-house development teams and the Docker and Kubernetes options provided by the vendors.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 360, 'parent\_id': '0041aab5296fff40465675df630925ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9984bf2c2e16c4993e795337d317312f', 'text': 'The Kubernetes API is the main mode of communication between the Kublet on the Kubernetes worker node and the Kubernetes API server. APIs are used by Kubernetes to create, configure, and manage the clusters.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 360, 'parent\_id': '0041aab5296fff40465675df630925ed', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '63d43f7c8339d86090f8e06f48c9fecd', 'text': 'Internal Interfaces', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 360, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ca7de9d7c337137e7f44948869b9cac1', 'text': 'Let’s first have a look at the internal container communication threat surfaces.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 360, 'parent\_id': '63d43f7c8339d86090f8e06f48c9fecd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dc4cd9818d53c61a418448ff1c3e1d13', 'text': 'Although the 5GC network functions are containerized and can be ideally deployed in a single server, that is almost never the case. The 5GC network functions would need to serve millions of users, and this requires multiple instances to be instantiated to serve the users. There are also multiple considerations such as the vendor you are choosing to use for user plane functions and control plane functions. Looking at the scenario in a couple of years after this book is published, you will have so many different vendors to', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 360, 'parent\_id': '63d43f7c8339d86090f8e06f48c9fecd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '11d8624cc03b355609b6ba1ec924b77c', 'text': 'choose from, especially in MEC use cases catering for ultra-reliable low- latency communication (URLLC).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 361, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c5b868aa78cff5a47abebc26e5f7c312', 'text': 'Figure 6-8 and Figure 6-9 illustrate some of the different threat surfaces due to the deployment types. In this example, part of the 5GC CNFs are deployed on the public cloud and parts of them are deployed on premises. 5GC CNFs deployed on premises have separate host servers for SMF, AMF, and NRF that can be from multiple vendors. PCF, UDM, and AUSF components are deployed in the public cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 361, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '199722c090338e4578910e466da923e7', 'text': "SBI Message Bus 5 ,,,,,,, T Insecure container 3 | UbM | AUSF i PCF networking J AP 5GC NFs deployed on public cloud 5GC NFs deployed on-premises = SMF AMF NRF % =D AP' = e Server A Server B Server C", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 361, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9e88d841fd5186c8651d5d392d2e2ab6', 'text': 'Figure 6-8 Insecure Inter-5GC NF API Communication', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 361, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd7cadb7dc23134b159abe2ea01c48f9b', 'text': 'Figure 6-8 shows the threats in the SBI-based communications used for internal communications between the 5GC network functions due to insecure container networking both on the premises and in cloud-deployed CNFs. As can be seen from the Figure 6-8, due to the multiple-server deployment on the premises to cater for the higher capacity, the API calls between the 5GC CNFs have to be handled through switches and virtual switches. Insecure interfaces between the switches and the unprotected API calls increase the risk of man in the middle (MitM) attacks. When deployed in the public cloud, the same SBI message bus using REST HTTP/2 API calls is used for communication between the 5GC control plane CNFs. The unprotected API communication', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 361, 'parent\_id': '9e88d841fd5186c8651d5d392d2e2ab6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'daef1445e3b3bc687e5d5685b7a7f306', 'text': 'between the containers is prone to MitM attacks. Figure 6-9 illustrates threats due to the hybrid deployment model of 5GC containers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 362, 'parent\_id': '9e88d841fd5186c8651d5d392d2e2ab6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '3d8faf820c006d5ef062cc9e4bd0594b', 'text': 'S —— SBI Message Bus [ 4 Exploit API a vulnerabilities i UDM AUSF PCF Attacker API 5GC NFs deployed on public cloud o — | 5GC NFs deployed on-premises =y SMF AMF NRF API -1 AP 1 [0 [T [0 Server A Server B Server C', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 362, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '62f4056564e2fc3d90d5adb6f0bde8d6', 'text': 'Figure 6-9 Insecure External 5GC NF API Communication', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 362, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5acc2fe6656d17a442c6134eaf65399c', 'text': 'Apart from the internal communication threats within the on-premises and public cloud deployment models, deploying containers in a hybrid model (that is, having some 5GC containers on premises and some on the public cloud) brings in new threat surfaces. One of the key threat surfaces is unprotected communication between the on-premises and cloud-deployed 5GC containers, as shown in Figure 6-10. The other threat surface is improper configuration of the access controls, which might lead to improper access privilege for users accessing the API calls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 362, 'parent\_id': '62f4056564e2fc3d90d5adb6f0bde8d6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a4e6b3dd127712235405641113eeee38', 'text': 'Web Critical 3rd pany Virtual Network Industry and Services Infrastructure Application Operator Enterprise Verticals developers Q\_ P b o-Q-o ( A)) 1 di o } | B e e e R e S e 8 = S (S E e = R API Network Exposure Function API Service Based Interface (SBI) B e S v l SMF i i MF NRF - . oo %% 5G Core Service Based Architecture (SBA)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 363, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '60e73a6ef339e11bce2359c85640a738', 'text': 'Figure 6-10 5GC Network Exposure Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 363, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b16f954d2eb1515a256e8d3cce3a3a2', 'text': 'Another threat surface for the 5GC control plane CNFs is the implementation of the new network function called Network Exposure Function (NEF), which facilitates the access of 5GC network functions to external applications created by third-party developers, as shown in Figure 6-10. The concept of an exposure function is not new to cellular technologies. In 4G technology, Service Capability Exposure Function (SCEF) was used to expose the 4G packet core capabilities for IoT use cases, event reporting, and so on. The key differentiator in 5G for the exposure function is the capabilities of the service-based architecture (SBA) of the 5GC control plane containers, which use RESTful', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 363, 'parent\_id': '60e73a6ef339e11bce2359c85640a738', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5d47ede77ff69d0daaf4b61f4226016b', 'text': 'API calls. This makes the exchange of information easier and enables innovation in the development of applications for 5G use cases. In other words, NEF can be seen as an evolution of SCEF. The key threat surfaces arising in implementations of NEF are mainly due to improper access control and improper implementation of APIs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 364, 'parent\_id': '60e73a6ef339e11bce2359c85640a738', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b7aed8b501355c025864beeeee19a50f', 'text': 'External Interfaces', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 364, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8572f989373930c34c85e8bf4f8b5160', 'text': 'Apart from the API-based calls in the 5GC control plane SBA architecture, there are other non–control plane communications required for the 5G network to operate and fulfill use cases seamlessly. Figure 6-11 illustrates the external components for the 5GC control plane, and Figure 6-12 illustrates external components for the 5GC user plane, which requires integration with external components.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 364, 'parent\_id': 'b7aed8b501355c025864beeeee19a50f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c45075d01fbde7179217c614ddb3da64', 'text': 'I E—— 5G Packet Core CNFs - Key Control Plane Functions L] Nudm Nnssf ‘ Nnrf Nnef ‘ E‘ Nausf Nsmf | Namf ‘ SCP AUSF ws e | e e e e e e e S UE NAS messages Access Network 5GC UP NFs deployed on MEC (public cloud / on-premises) Non-5GC NFs deployed on MEC (public cloud / on-premises) Roaming Partners \* o o o o o Integration with enterprise non-3GPP NFs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 364, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd6217c9c74104ddaafe0ed46302d9200', 'text': 'Figure 6-11 5GC Control Plane Integrations with External Network Components', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 364, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '756574f44c16311c97a277952d0c6b4e', 'text': 'Components', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 364, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'b74e566b35ae286cf21fefb3efbdce46', 'text': '5G Packet Core CNFs - User Plane UPF e e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 365, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cecf76bdb238bcc64aa8c479fcdd8064', 'text': 'Access Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 365, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '197afdeec1080cfae98b72986f32d168', 'text': 'o', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 365, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2d89f4fe6cf4ae14540f39f94b86ad35', 'text': 'o', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 365, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '797c03bbba9f4b5ee1481fb5f2b346ef', 'text': '5GC CP NFs deployed on public cloud / central DC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 365, 'parent\_id': '2d89f4fe6cf4ae14540f39f94b86ad35', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8332f60e827402826b8ca1832d65d6f0', 'text': '5GC UP NFs deployed on public cloud / central DC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 365, 'parent\_id': '2d89f4fe6cf4ae14540f39f94b86ad35', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ba3b1cb8d26c3914b6fc805f9a698ac4', 'text': 'o', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 365, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d2e07c9bd8db7a21386bb435a3d693a', 'text': 'Non-5GC NFs deployed on MEC (public cloud / on-premises)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 365, 'parent\_id': 'ba3b1cb8d26c3914b6fc805f9a698ac4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'ListItem', 'element\_id': 'e16bc33243e0680b452fe1c9e9538ead', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 365, 'parent\_id': 'ba3b1cb8d26c3914b6fc805f9a698ac4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2060465e81218066111c7dc4e8903ce7', 'text': 'Integration with Enterprise DC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 365, 'parent\_id': 'ba3b1cb8d26c3914b6fc805f9a698ac4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1023b7d290c8c9818781e39f31745206', 'text': 'Figure 6-12 5GC User Plane Integrations with External Network Components', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 365, 'parent\_id': 'ba3b1cb8d26c3914b6fc805f9a698ac4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a89861d844c15c67e94f56bb6a53e26c', 'text': 'Traffic between the containerized 5GC network functions is normally routed over a virtual overlay network that is managed by the container orchestration platform and usually bypasses the network security and management layer within your organization. This becomes an issue when the traffic between the containers are encrypted. Existing network security controls in your network will not be able to provide visibility into the actual container communications, and it’s not ideal technically and commercially to deploy a decryption engine between each and every container. This causes a lack of visibility in your container environment and ineffective monitoring of your network traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 365, 'parent\_id': 'ba3b1cb8d26c3914b6fc805f9a698ac4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b1cde877904c89bb1dfe9a32f96cfdbe', 'text': 'This opaque network layer caused by encrypted inter-container traffic becomes critical if you have a mix of critical applications and Internet-facing web applications share the same virtual infrastructure. You will face this issue when containerized 5GC functions are deployed along with non-3GPP 5G applications in the MEC layer, as shown in Figure 6-13.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 365, 'parent\_id': 'ba3b1cb8d26c3914b6fc805f9a698ac4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '31e53995546db61a0339a6a5ee81eb69', 'text': 'pratabe et B b Internet Comaingis R % Undetected malware exposed to critical < Containerized Internet- containers S facing application . ﬁ 5 Host OS Host OS Encrypted traffic « between containers B B L2/ L3 Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 366, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '10736a8c8c86fef69c225baac943f4c5', 'text': 'Figure 6-13 Impact of Compromised Web-Facing Application', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 366, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd1e332e3c18efd1ae4a62bf75bc173f1', 'text': 'Figure 6-13 illustrates how a compromised containerized web-facing application could impact the critical container sharing the same virtual infrastructure. The communication between the containers is encrypted with methods such as Transport Layer Security (TLS). While the communication is passing through the L2/L3 network, which could be a virtual switch deployed on the infrastructure, the traditional network filters would see only the encrypted packets between the two hosts, without any visibility into the traffic between the container endpoints. If the web-facing application is infected, any malware being sent using the encrypted path would be invisible to you.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 366, 'parent\_id': '10736a8c8c86fef69c225baac943f4c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0130df99992f07c72c4152923889d778', 'text': 'Figure 6-14 illustrates the roaming interfaces of the 5G non-standalone architecture (NSA) and different integrations required between the home public land mobile network (PLMN) and visitor public land mobile network (VPLMN).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 366, 'parent\_id': '10736a8c8c86fef69c225baac943f4c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c93d2bc480b7af00f4eb7611e39b13e1', 'text': "HSS + UDM Eq N8 N7 — hPCF EGW’C +SMF HPLMN Séa $8.C N16 4y PGW\_U + UPF N9 B —— N8 GTP-U N24 ulnerabillli\\ 4s8.u API <l I > o e - vulnerabilities @ Diameter & GTP-C SGW UPF] VSMF vulnerabilities VPCF 4 CIRES N11 N15 N26 AMF VPLMN @MME $1-C §1-U N3 Nz¢ <'\\AN1 - U e ((A)) eNB ( A)) NF!-.U'u gNB", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 367, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '176ad9cfe7e97c318350cb264c391641', 'text': 'Figure 6-14 Roaming Interface for NSA and SA Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 367, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f21cac70757da1c3fc9702ab31387ee7', 'text': 'As shown in Figure 6-14, NSA deployments have to cater for the integrations between the 4G Evolved Packet Core (EPC) and 5GC network functions for roaming scenarios. The control plane vulnerabilities of GTP (control plane and user plane) and Diameter protocols are well-researched areas, and the attack vectors are well documented. For the 5GC integrations, the following reference points would use API calls in a roaming scenario:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 367, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '68564e5f7123e43ffaf3041147e7fc1f', 'text': '• N8: Reference point between VPLMN AMF and HPLMN UDM', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 367, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e208390ae06f51a266cf15f203b22497', 'text': '• N16: Reference point between VPLMN SMF and HPLMN SMF', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 367, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '567dfea2459ee278409ae0703a4030bb', 'text': '• N24: Reference point between VPLMN PCF and HPLMN PCF', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 367, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da67f460cb1945a629cfd1b4a52cc14f', 'text': 'These interfaces (N8, N16, and N24) are susceptible to attacks exploiting the API vulnerabilities due to improper API implementation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 367, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b34fb65cb5ae662e76cde0799f7dab6f', 'text': 'Orchestration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 367, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd826311d3cc1e477bb4ae6ffb6016d79', 'text': 'Containerized 5GC network functions, whether on the premises or in the public cloud, will be dynamic in nature and should have the capability to maintain state, which is very important to ensure high availability and provide services', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 367, 'parent\_id': 'b34fb65cb5ae662e76cde0799f7dab6f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6b9d2bb8c198468cbd88b54ad703f734', 'text': 'to your 5G subscribers and use cases. This capability is provided by the orchestration layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 368, 'parent\_id': 'b34fb65cb5ae662e76cde0799f7dab6f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c1c16a5144bc1a6f33295d30c6d18f1e', 'text': 'This makes the orchestration layer one of the key targets for attacks. The orchestration layer usually manages thousands of containers and is designed to handle multiple users. This brings in one of the key threat surfaces of improper authentication and authorization of users accessing the orchestration platform. Figure 6-15 illustrates the risk of an attacker having unauthorized access to the orchestration platform.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 368, 'parent\_id': 'b34fb65cb5ae662e76cde0799f7dab6f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '171f4080a53731e9d057c4ae0f012f9e', 'text': 'P ——— Container { Orchestration E - cecmcmcmanans, i -, mfommmm e, NN~ JE— :E ;\\ :; Container Repository Public Cloud 5GC Container cluster Container i: Orchestration 3 Exploit API ,,,,,,,,,,, [ommm————— vulnerabilities in i U F—— Orchestration 0 [ . Attacker On-premises 5GC Container cluster', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 368, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '76aaee580fa354472109dcd61be09bf5', 'text': 'Figure 6-15 Attacker Having Unauthorized Access to Orchestration Platform', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 368, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '62e0928316d473784214ef11fdb3b249', 'text': 'Container orchestration platforms normally allow every application access to query the API. Container orchestration platforms use a role-base access control (RBAC) that integrates with an external authentication directory such as Lightweight Directory Access Protocol (LDAP) or an existing authentication', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 368, 'parent\_id': '76aaee580fa354472109dcd61be09bf5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd554d71857f9809fd726e868b5b3afd9', 'text': 'solution being used by the specific teams operating the packet core, which is separate from the user directories used by your IT department or organization. Having multiple authentication solutions is quite common with service providers where one or more authentication solutions are implemented per department. This leads to an isolated directory system that is prone to weaker management and improper access control. The container orchestration platform usually caters for managing containers with high privileges. If the authentication directory within such orchestration platforms is misconfigured or not properly audited and managed, the permissions will be escalated quickly, consequently allowing the attacker to inject malicious code into the 5GC network functions or deploying a container with malicious code in it. Once the attacker performs privilege escalation, they could destroy the legitimate 5GC containers and cause disruptions or an outage of your 5G network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 369, 'parent\_id': '76aaee580fa354472109dcd61be09bf5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a562480bbcf0e841ead47b8d33a713c4', 'text': 'Another area of risk in the container orchestration layer is unauthorized hosts joining the container cluster. Improper configurations on the orchestration platform can lead to unauthorized access and unauthorized host configurations, which can expose the container clusters to increased risks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 369, 'parent\_id': '76aaee580fa354472109dcd61be09bf5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9e6d185cf7f60467ba70e9f0debaa03f', 'text': 'Container Host and HW Vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 369, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c19f04ffa2f5e94867dae87518f15b8d', 'text': 'The previous sections covered the vulnerabilities and risks in containers, container networking, and orchestration. The underlying host introduces new attack vectors, which are further discussed in this section. One of the key attack vectors is exploiting the CPU optimization methods used for code execution, and the range of attacks is aimed at applications running on same core. There are also other attack vectors due to insecure supply chain, such as changing the design of the circuit board to include malicious chipsets or shadow chipsets. Apart from malicious chipsets, the legitimate off-the-shelf chipsets also have risks such as unauthorized read/write access to their virtual memory, which can lead to leakage of cryptographic keys. These malicious chipsets and vulnerabilities within off-the-shelf chipsets could be used to execute the load instructions before the legitimate CPU gets them. Many chipsets available today have micro-codes embedded into the firmware for management. These micro-codes are found to be vulnerable, enabling attackers to have root access leading to data from encrypted hard disks being decrypted, device IDs being forged, and even the ability to extract digital content. Other attacks, such as Spectre and Meltdown, exploit the read/write implementations of the chipset manufacturer, leading to exfiltration of data. Critical vulnerabilities and threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 369, 'parent\_id': '9e6d185cf7f60467ba70e9f0debaa03f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ff252c96566ce66a128ec6db02f2be11', 'text': 'attacks related to the hardware vulnerabilities are explained in the “Hardware and Software Vulnerabilities” section in Chapter 5.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 370, 'parent\_id': '9e6d185cf7f60467ba70e9f0debaa03f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'daebb86e4cd048a8efa6150a747323b2', 'text': 'The main issue in deploying 5GC Cloud-Native Functions in the public cloud is the hardware used by the public cloud providers for hosting your applications. If the hardware used by the cloud vendor uses chipsets that are insecure, the cloud provider’s DCs are already exploited, and your data is not safe from the time it is deployed in the compromised cloud provider’s environment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 370, 'parent\_id': '9e6d185cf7f60467ba70e9f0debaa03f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'efcc7333c0244c6b75b81d8b947e2ed3', 'text': 'One of the key areas of concern while deploying the 5GC containerized network function in the public cloud or on-premises data center is the level of isolation provided during deployment. Containerized 5GC functions can be deployed on VMs or bare metal. Many vendors today are offering bare-metal container deployment options, but they need proper validation to ensure that the container environment provides proper isolation. Let’s discuss some of the isolation issues related to container deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 370, 'parent\_id': '9e6d185cf7f60467ba70e9f0debaa03f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a4116b0489e13cc5d4c802279c2d192e', 'text': 'When 5GC network functions are deployed as containers on virtual machines, they use the VMs as the host operating system rather than running directly on bare metal. VMs provide inherent isolation between the VMs and host operating system, as illustrated in Figure 6-16. A container-on-VM deployment is one of the key methods used by public cloud providers to enhance the isolation between your 5GC network functions deployed on cloud and the other customers’ applications deployed on VMs or containers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 370, 'parent\_id': '9e6d185cf7f60467ba70e9f0debaa03f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5b9ea811516b19c551f6349eb5dc7f45', 'text': 'No inherent isolation Inherent Isolation provided Inherent Isolation provided by virtual machine for container deployment provided by bare metal by virtual machines deployment for containers Virtual Machine Containers A FE < S /\\ G — AMF F UPF R e e s e SM Al M F|| SMF = | & | MF SMF UP =] ) g Container Container Guest OS ¢ Runtime Runtime i | Gueet 05 | Container Runti ime Hypervisor S Host 0S Host OS nfrastructure A= % & nfrastructure i ) | 5G CNF as VM 5G CNF as Containers on VM 5G CNF as Containers on BM', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 371, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c7537e2c57673087bd0581791c6d7844', 'text': '5G CNF as VM', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 371, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '868ddd0a2ca1d98b91c2fc09383cc89f', 'text': '5G CNF as Containers on VM', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 371, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e122babaa79f770c9a99c1348ad63792', 'text': '5G CNF as Containers on BM', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 371, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '15de2260c50cde30a066df62982fb549', 'text': 'Figure 6-16 Isolation Provided by Different 5GC CNF Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 371, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4102d3e008e2f74f01298b69ce97ae95', 'text': 'Isolation is not the only consideration you will have before choosing the deployment option. If you have a colleague from the data center compute team working with you for the dimensioning part, the criteria would be consumption of computing resources, such as memory, storage, and CPU, which is very efficient in containers deployed on bare metal. Another aspect could be ease of operations and maintenance, which are again better handled by deploying containers on bare metal. Containers on bare metal also help with the ease of deployment and scaling, as they are deployed on a single operating system (OS), which reduces the number of OSs that need patching and so on. All these benefits of deploying containers on bare metal will lead to you choosing this option over containers being deployed on VMs. But in pragmatic network deployments, you might actually end up using containers on VMs and BMs, as shown in Figure 6-16.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 371, 'parent\_id': '15de2260c50cde30a066df62982fb549', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f13bd71b1462a90c0fc1f656e3983089', 'text': 'A containers-on-BM deployment is chosen where latency is critical to enable ultra-reliable low-latency communication (URLLC). These deployments would be typical at the RAN site location or at the far-edge DC, as shown in Figure 6- 17. In other locations, such as the MEC and central DC, you can deploy containers on BM or VMs. Let’s therefore take a deeper look into the insufficient isolation in bare-metal deployments and their vulnerabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 371, 'parent\_id': '15de2260c50cde30a066df62982fb549', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'e68e472f566620d79adee2547cb88e1f', 'text': "———— Preferred mode of ontainers on! { Containers on | | :rContainers on! container deployment : 'BM/ VM | BM/VM 5GC Control Plane CNFs 5GC User Plane CNFs F T C —— LSBT 1 — S ., ————— S — - ----- 1 = ((A>) =] Central DC - On-prem Radio MEC - Node location On-prem DC or Public Cloud On-prem DC or Public Cloud", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 372, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '428172a9aa7a544280e002ae39dc9190', 'text': 'Figure 6-17 Preferred Mode of Containerized 5GC Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 372, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd33f6f77dafb695493d81ebf8bfb56f8', 'text': 'Containers allow you to package your 5GC network functions and its dependencies together in a single object. The isolation for containers is provided by namespaces, which define the boundary by partitioning kernel resources for a process. For some use cases, such as running processes that require direct hardware access such as read/write access to the root partition, some containers can be run as privileged. For example, in Docker, “-privilege” is a special flag that you can set at runtime specifically to allow a Docker container to break free from its namespaces and access the entire system directly. It is just like you having access to the host machine. This can be exploited by the attacker, as shown in Figure 6-18.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 372, 'parent\_id': '428172a9aa7a544280e002ae39dc9190', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c7e6f81630e442ef9d86d5147b48d609', 'text': '@ a Attacker AM UP App 1 Host OS . Infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 373, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '949f2419a485c5c8cd5bbf5d0be25f49', 'text': 'Figure 6-18 5GC NF Being Impacted Due to Privilege Escalation Type Attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 373, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3708ba0e852351ead8208ce0860ab696', 'text': 'The attack vector shown in the Figure 6-18 follows these steps:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 373, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ad43c9e97598be2fe4b13da48140ad9c', 'text': '1. The malicious application deployed in your container environment is run as privileged.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 373, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '55a2febc85c6fcac21981df8047dfc38', 'text': '2. Once the malicious container of the attacker is run as privileged, it can allow malicious code from the attacker’s container to overwrite or modify the SSH keys to allow remote users to log in to your container environment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 373, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '949bba689904c2ded07eb9a4bb7ef09d', 'text': '3. The malicious code then proceeds to destroy the AMF, SMF, and the UPF 5GC CNFs, thereby causing outage and service disruption in the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 373, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1b8f9edcfc60790d66499839060d8215', 'text': 'In another version of the attack, the attacker can use the container escape using the “-privilege” flag. This is an attack seen when the containerized network function that needs to have host resources from the container environment is given a “-privilege” flag. If an attacker can gain control over this containerized network function, they can escape the container environment and access the root privileges.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 373, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7ca130e333c2e43e30642cf3458c361d', 'text': 'The scenarios illustrated in Figure 6-18 should be carefully considered when deploying 5GC containerized network functions in an enterprise environment in MEC use cases. The enterprise environment will have many built-in container applications and third-party applications already deployed in the enterprise data center. If the 5GC containerized network functions are deployed', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 373, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8184e4473f028293e7550957e7bcb5da', 'text': 'in the same virtual environment as that of the third-party applications, some with the “-privilege” flag, the container escape attack by an attacker can destroy the critical applications, causing data exfiltration and denial of service (DoS) attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 374, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3d77963c0aea55ba756c6d0e7c885055', 'text': 'Improper Access Control', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 374, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd47e5f6f45fa70f39e81e9a600845a91', 'text': 'Figure 6-19 illustrates the access control provided by traditional segmentation methods used in legacy networks like 4G and 3G. The traditional network segmentation methods are based on IP address and ports. IP address are very important to traditional network security controls, as the network is segmented based on the IP and port information. When this information is coupled with user context, you can have policies that map users to an IP address or pool of IP addresses. But in a cloud-native deployment, IP addresses are not very helpful because they are very dynamic in nature and hence not considered the best way to apply security policies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 374, 'parent\_id': '3d77963c0aea55ba756c6d0e7c885055', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '4a711e38d51769322db74ca6153c54c7', 'text': 'e £ User u l 5G MEC Public Cloud Policy based on Traditional A Segmentation methods | s, Policy basea ;n IP [ address & ports 0 ] . 5G MEC on-premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 374, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '49a679bdb4b4789521834ad737b4f69a', 'text': 'Figure 6-19 Access Control Based on Traditional Segmentation Policies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 374, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '25a8b47592a13465aa0730878ca33466', 'text': 'Another issue with the traditional access control mechanism is that there is no stickiness to the policy, as illustrated in Figure 6-20. It means that there is no flexibility in moving the policy along with the 5GC NF workload when you migrate it from on-premises to public cloud. Although methods like role-based access control (RBAC) can be used to restrict system access to only authorized users, the main aim of RBAC is to provide access to a wide range of range of users.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 375, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ce07e6c07a685c10ec68ddb1e9c3ab7d', 'text': 'No Policy migration gl N s T 5G MEC Public Cloud o L / 5G MEC Public Cloud / Py 1 I (] I Migration of 5GC workload -] from on-premises to public [0 cloud 5G MEC on-premises 5G MEC on-premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 375, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e62f438743f7193cad2e65a5e19d1513', 'text': 'Figure 6-20 Lack of Policy Stickiness Using Traditional Segmentation Methods', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 375, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1b0dd6bdea40b8b447846bd992c79c9b', 'text': 'Securing Virtualized 5G Packet Core Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 375, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c64b1069ff82669e0d89e1bce3684cc1', 'text': 'Securing virtualized 5GC NFs that follow the cloud-native approach requires a new mindset toward securing your 5GC environment. The key areas of discussion in this section are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 375, 'parent\_id': '1b0dd6bdea40b8b447846bd992c79c9b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '77485d8bad11c17ee978628b0f6878b4', 'text': '• Secure CI/CD', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 375, 'parent\_id': '1b0dd6bdea40b8b447846bd992c79c9b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4d6cff3540c01ee9e0327c1cf15ba57a', 'text': '• Securing 5GC NF runtime', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 375, 'parent\_id': '1b0dd6bdea40b8b447846bd992c79c9b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7eb74d3af91848bb98eb246c6a576c01', 'text': '• Securing 5GC NFs and 5GC NF traffic', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 376, 'parent\_id': '1b0dd6bdea40b8b447846bd992c79c9b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f54e542a04fb168bac70e715a3fea88a', 'text': '• Securing 5GC NF orchestration and access controls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 376, 'parent\_id': '1b0dd6bdea40b8b447846bd992c79c9b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3a9077a648e1b985002e97504e0164ea', 'text': '• Securing 5GC NFs in roaming scenarios', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 376, 'parent\_id': '1b0dd6bdea40b8b447846bd992c79c9b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '744c96741c82187c177f64eed08edd5c', 'text': '• Securing host OS and hardware', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 376, 'parent\_id': '1b0dd6bdea40b8b447846bd992c79c9b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d6549b1980345b523773048d855d769', 'text': 'A majority of service providers are planning to deploy container-based virtual 5GC NFs. This section will discuss the aforementioned key discussion areas in much more detail.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 376, 'parent\_id': '1b0dd6bdea40b8b447846bd992c79c9b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b4efa3954da3f7be26b784c5e767fcbd', 'text': 'Secure CI/CD', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 376, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ad22b79e08ef45895c0a925128556740', 'text': 'The Continuous Integration/Continuous Delivery (CI/CD) process, as covered earlier in the chapter, is very crucial to the software development lifecycle. It includes code and image repositories, build servers, containers, and third-party tools. CI is a process where software developers merge software code. CD is a process that includes provisioning the infrastructure for container deployment. Figure 6-21 illustrates the high-level stages of a CI/CD process.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 376, 'parent\_id': 'b4efa3954da3f7be26b784c5e767fcbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '803ce94ff8f550317495520b8dfd43f7', 'text': '= Continuous Integration Continuous Delivery', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 376, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '14697223c08748c07e9073d0960f38b1', 'text': 'Figure 6-21 Stages of CI/CD Process', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 376, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fa3bb6405fa01fd53675a8fc5d535c7a', 'text': 'Securing CI/CD would require close integration between the DevOps process and the container security controls. Such integrations are also called DevSecOps. Using DevSecOps will help you to automate the container security checks, thus ensuring trusted images are deployed to runtime and are monitored for anomalies once deployed in production. This should be followed by the vendors’ development teams developing containerized 5GC network functions or by teams developing applications that would interact with the 3GPP 5GC containerized network functions, as illustrated in Figure 6-22.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 376, 'parent\_id': '14697223c08748c07e9073d0960f38b1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ab08a39c192c7db38926a4aaf531e423', 'text': "Scanning for any vulnerabilties in the 5GC Containers deployed in public cloud scanned for open-source components used for any vulnerabilities and building containerized 5GC network anomalies in container functions behaviour .m Q/’ A Developer Container registry A Any found vulnerabilties is scanned for any and anomalies found have to be corrected and unsigned images ] modified by the development process 5GC NF deployed in pum— . ‘ /' public cloud » . ™~ D — ‘/% %/{@ e 5GCNF Scanning for any ] vulnerabilities and anomalies image build in the image build and st o] deployment scripts Image signed before 5GC Containers deployed in on- =B being uploaded to the premises datacenter scanned for 5GC NF deployed container registry any vulnerabilties and anomalies in container on-premises behaviour", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 377, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b956f2c8f8c5832aef4de67eb2b25d19', 'text': 'Figure 6-22 Secure CI/CD Process', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 377, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8294a2c52149560b3355321aa1512097', 'text': 'Some of the key integration points illustrated in Figure 6-22 are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 377, 'parent\_id': 'b956f2c8f8c5832aef4de67eb2b25d19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e8d662feb90d6c162d9bb7f3212de53', 'text': '• Continuous scanning: The scanning should include container build and deployment. Continuous scanning should be implemented throughout the CI/CD process to identify any issues related to misconfiguration (intentional/unintentional) in the deployment scripts. The scripts should be scanned for any keys, credentials, and secrets. Any such details found should be removed and be protected by trusted secret managers. 5GC CNF will include open source components for the images. These images should be scanned continuously for any vulnerabilities—during development, while being moved into production, and during production.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 377, 'parent\_id': 'b956f2c8f8c5832aef4de67eb2b25d19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ddf71289bf7354e942b24a8aa006349b', 'text': '• Continuous monitoring: The expected behavior of the 5GC container should be modelled and any identified anomalies from the expected behavior should be identified and an alert created for the security teams to ensure deeper investigation, if required. There are many options available today to have automated monitoring of container behavior.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 378, 'parent\_id': 'b956f2c8f8c5832aef4de67eb2b25d19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e321938b00e7ca37e3d19a637a67b739', 'text': '• Image configuration: Improper configuration is one of the key challenges in configuring containers apart from compliancy. You should ensure that the images are configured to run as non-privileged users. Many of the 5GC containerized network functions come with vendor-specified recommendations. Any methods for remote users, such as SSH, should never be enabled. Only API access should be allowed for any remote management.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 378, 'parent\_id': 'b956f2c8f8c5832aef4de67eb2b25d19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '72161b9d5908cac80b28f21308298eb7', 'text': '• Secure registry and include image signing: A container registry such as a Docker registry is a kind of repository for developers uploading container images. This is a very useful concept because it enables providing the most up-to-date images with all the vulnerabilities patched in one location. The key issue, as explained in the “5GC Container Vulnerabilities” section earlier in the chapter, is the attacker exploiting known vulnerabilities and modifying the images with obsolete code or malicious code that can be executed in your production environment. The other risk is the attacker scanning the registry for any vulnerable or insecure API implementation that can then be exploited by the attacker. To offset these issues, container registries these days use the concept of a trusted registry, such as Docker Content Trust, that implements The Update Framework (TUF), which uses the online/offline key concept, where the offline key is stored securely and used to sign the timestamp key and tagging key. To secure the image, you should have the visibility of the entire 5GC container lifecycle, from the build process to signing the image before being uploaded to the registry, to visibility during runtime to detect any anomalies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 378, 'parent\_id': 'b956f2c8f8c5832aef4de67eb2b25d19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f2cbeacb4a9a65d7f2f5a0362d38ce8d', 'text': '• Securing 5GC NF runtime: Securing container runtime means securing the container application environment, which includes analysis of the container and host activity as well as monitoring the protocols and payloads of the network connections. Having a secure runtime would require integration with the CI/CD pipeline.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 378, 'parent\_id': 'b956f2c8f8c5832aef4de67eb2b25d19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2f534b3e6fe66a36b781c26048c81e81', 'text': '• Unique identity for each workload: This method involves creating a unique identity for each workload early in the CI/CD pipeline and then', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 378, 'parent\_id': 'b956f2c8f8c5832aef4de67eb2b25d19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67deaf5320c90ece3e0e31e50e9b4bab', 'text': 'using these identities to enforce security policies on the clusters, thereby preventing unauthorized hosts from being deployed and communicating with legitimate workloads, as shown in Figure 6-23. This method would require interaction with the 5GC vendor building the network functions and the service provider deploying the container.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 379, 'parent\_id': 'b956f2c8f8c5832aef4de67eb2b25d19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a3bfe2f88833f221e2407c63e884b016', 'text': "Secure 5GC Container Runtime Platiorm ' T o A Developer Create Unique ID for each Workload to security [ 5GC workload created policy mapping I [} Apply securiy policy related to the workload f 5GC NF deployed in pr— . public cloud - g (o), ; ™~ é\\ e | 5GCNF image build 7] [ 5GC NF deployed on-premises", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 379, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'fe8d80bfe1a491437cb88df6e11dbdfa', 'text': 'Figure 6-23 Secure 5GC Container Runtime', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 379, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd8ff0d3b8ee34119ffaae10e1c64c690', 'text': '5GC CNFs being deployed as containers will require authentication and encryption of the inter-5GC container communications as well as external communications. TLS should be implemented to ensure that inter-5GC control plane network functions are secured. 5GC control plane network functions uses service-based architecture (SBA), which implements a service-based interface (SBI) using RESTful APIs based on HTTP/2. RESTful APIs are also used by the Network Exposure Function (NEF) for capability exposure to third-party application providers and integration with industry verticals enabling 5G use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 379, 'parent\_id': 'fe8d80bfe1a491437cb88df6e11dbdfa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c3254eeb171490857e66885a5ca0b01a', 'text': 'Although API communication facilitates integration between 5GC NFs, API vulnerabilities are well known by the attackers, consequently increasing the vulnerability of your network. The security controls illustrated in Figure 6-24 and described in the list that follows will help secure your 5GC NF’s communication at runtime.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 380, 'parent\_id': 'fe8d80bfe1a491437cb88df6e11dbdfa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '24cf1dc027dd84070bcf7861f1d05d64', 'text': 'API GW / WAF to mitigate = attacks exploiting API vulnerabilities mTLS Analyzing encrypted traffic for malware without decrypting the traffic API GW | WAF . 5G Packet Core CNF i e e e i UDM NSSF NRF EF PCF iJ Nudm | Nnssf | Nnrf Npcf] afE Nnef] aust i Nsmf | Nam! AMF e o e e e e s el s el St s Tt Use SCP (optional 3GPP) for creating NF <> NF communication mapping and high- level global access list etc', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 380, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b2e0a5b725b8bea735f2037b400d0df5', 'text': 'Use SCP (optional 3GPP) for creating NF <> NF communication mapping and high- level global access list etc', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 380, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '016823a43b018016888d74011bc216c2', 'text': 'Figure 6-24 Security Controls to Secure 5GC NF Runtime', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 380, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dc8490d4018c9bef669743e50b2395e5', 'text': '1. Service communication proxy (SCP): SCP is defined in the 3GPP TS 23.50, Release 16 specification for system architecture for the 5G system. It is not a mandatory feature/component of the 5GC. SCP will enhance the 5G network function service discovery and selection process by enabling and managing the 5G NF-to-NF mapping. It can also implement access control lists to prevent unauthorized communications between NFs. SCP also provides cryptographic verification using authentication mechanisms like', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 380, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d3b0e2892205544030bffdfe4ef3802', 'text': 'mutual Transport Layer Security (mTLS), which is an extension of TLS, between the SCPs and the NFs and between SCPs within the PLMN.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 381, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd125ef37ecf4322a7cc6355e397d1c9d', 'text': '2. TLS/mTLS: All 3GPP NFs has a mandatory requirement to support TLS, which should be used if other means of network security such as Network Domain Security (NDS) using security gateways (SecGWs/SEGs) are not implemented in the 5GC PLMN network. The protocol stack for the SBI is illustrated in Figure 6-25. Any vendor you choose for the 5GC deployment should support TLS/mTLS within the 5GC NFs. This will ensure that you can enable TLS to secure the 5GC NFs when you want to implement it later in the deployment stage. It is recommended to use TLS 1.3 because it provides a faster, simpler, and more secure cipher suite, thereby providing better performance and enhanced security as compared to its predecessor, TLS 1.2.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 381, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '9282e36162b1a375dc4ab48187a5a531', 'text': 'Application HTTP/2 TLS TCP P', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 381, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fa60dae4214ab1b24013c3f2048ce244', 'text': 'Application', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 381, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '30915001b275cb662f54500f68ca17fb', 'text': 'HTTP/2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 381, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '93d5ea39b63288ca8d228cfc88c41e4b', 'text': 'TLS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 381, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '376e7edaf6c17c3f2a0fe4c76e3ddd90', 'text': 'P', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 381, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7fae977bb15bdcb8277530a6cc333365', 'text': 'Figure 6-25 Service-Based Interface Protocol Stack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 381, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b7076ab0fa984b79b39a8a35806a3470', 'text': '3. API GW/WAF: TLS is used to provide integrity, replay, and confidentiality protection for the interface between NEF and AF network functions. Once authenticated, the NEF will determine if the AF is authorized to send requests toward the 3GPP 5GC network function. This authorization is performed by using the OAuth 2.0 authorization framework, as specified in the IETF RFC 6749. The Common API Framework (CAPIF) can also be used for interactions between NEF and APF. CAPIF is discussed in the section “Securing API” in Chapter 5. Due to improper implementations of the API, most of the API calls from the third-party Application Function (AF) and any MEC application to the Network Exposure Function (NEF)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 381, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '544d9164cacac3eee5ff522713a6cc6f', 'text': 'are vulnerable to API risks. To mitigate any risks from vulnerable APIs or improper implementation of the APIs, it is recommended to use the API gateway (API GW) or a web application firewall (WAF). An API GW or WAF would protect the 5GC components from any attacks, such as cross- site scripting (XSS), SQL injection, and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 382, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dea858396ebae12933b0412255e289ae', 'text': '4. Analyzing encrypted traffic: TLS communication between the 5G NFs and between 5G NFs and AFs enables enhanced privacy and security for use cases by using keys and certificates to ensure security and trust. However, service providers and enterprises are not the only ones to benefit from encryption. Threat actors have leveraged these same benefits to evade detection and to secure their malicious activities. Some categories of threats that use encrypted traffic are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 382, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aff3a3fb91bd338a06411bbe3980205a', 'text': '• Illicit crypto mining', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 382, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b59b8a16ef4c593291a218efc9c52f6c', 'text': '• Android OS Trojans', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 382, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '23391ac1666517cba7e760abdd249abe', 'text': '• Ad injectors', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 382, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd1e934754005fb07927c684aff1f9d48', 'text': '• Sality malware', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 382, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '39c87c2f8b186d14704b9e8220fb7aa5', 'text': '• Malware using SMB (Server Message Block) service discovery', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 382, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '68bda9b1b12130b6456e786675b869a6', 'text': '• Potentially unwanted applications such as Tor and BitTorrent', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 382, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d3298c11077c08b17d19b4e08ca73a8', 'text': 'Traditional threat inspection with bulk decryption, analysis, and re-encryption is not always practical or feasible for 5G use cases due to performance and resource reasons. Also, it compromises privacy and data integrity.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 382, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5d99e7a6fb3f0918d7d5c43ad2e2187e', 'text': 'Today, a couple of solutions providers from cybersecurity vendors focus on identifying malware communications in encrypted traffic through passive monitoring, the extraction of relevant data elements, and a combination of behavioral modeling, artificial intelligence, and machine learning with cloud- based global visibility. The solution you choose should analyze the new encrypted traffic data elements in enhanced NetFlow by applying machine learning and statistical modeling, as shown in Figure 6-26. Rather than decrypting the traffic, the solution should use machine learning algorithms to pinpoint malicious patterns in encrypted traffic to help identify threats and improve incident response. Upon discovery, the malicious encrypted traffic should be blocked and quarantined to an isolated and segmented network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 382, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8e51b528ab0674419dfe4ea32330d07e', 'text': 'The solution used for analyzing encrypted traffic should identify encryption quality instantly from every network conversation, providing the visibility to', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 382, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5ba74cb34c5b45230f09e84f34be7828', 'text': 'ensure enterprise compliance with cryptographic protocols, as shown in Figure 6-26. This will enable you to identity any noncompliant cryptographic protocol implementations in the network and take corrective actions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 383, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '646d1b5da0cf99fe0821c615a9326317', 'text': 'Packet Header details, src IP, dst IP etc Cloud based Al > &ML Engine Packet header extraction and analysis device o e —————— 0 = Indicates malicious traffic within encrypted traffic (no decryption required) ) (- [Lee ) Aggregated AP| calls o AP calls L2/L3 secured == Data Center secured device with TLS Data Center Server with TLS Server', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 383, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '83b8f581d0dc31c5fb3177da95382f25', 'text': 'Figure 6-26 Detection of Malicious Traffic in Encrypted API Calls Without Decryption', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 383, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c882bc3c736c0a8855f49204c0841e2e', 'text': 'Figure 6-26 shows one of the methods to detect malicious traffic within encrypted traffic without decrypting it. This method shows additional telemetry from routers and switches specifically related to encrypted data. The AI and ML engine in the cloud then analyzes specific details collected and determines whether the encrypted traffic between the 5GC NFs or between the 5GC NEF and the Application Function contains any malware. This would enhance the security in the 5GC virtualized deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 383, 'parent\_id': '83b8f581d0dc31c5fb3177da95382f25', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a276428078ed05781cfc620bd90f8571', 'text': 'Securing 5GC NFs and 5GC NF Traffic', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 383, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '452c34a833ab63ba6075a3a8ace18f3b', 'text': 'Most vendors are proposing container-based deployment (VM based and BM based) to make full use of virtualization technology. To secure 5GC NFs, security controls should be closely mapped to the workloads themselves, moving with the instances and data anywhere they might run (in data centers, virtual infrastructure, or cloud environments). Using this method, you will have', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 383, 'parent\_id': 'a276428078ed05781cfc620bd90f8571', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '82f4089e29f5c17fae977d0e268893b0', 'text': 'a much stronger chance of protecting data regardless of where the system runs. The actual behavior of the applications and services as well as the mapping of applications and services also need to be catered for to enable the right security controls to the right applications, which requires granular isolation between specific workloads, regardless of the environment in which they are deployed. This requires a new mindset for securing the network, as illustrated in Figure 6- 27.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 384, 'parent\_id': 'a276428078ed05781cfc620bd90f8571', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c49fecb0ea1ab5bb44903e51c4e72651', 'text': 'Micro - segmented Customized 5GC NFs L= security policy b e ] L] of=i ) 0 0 5G MEC Public Cloud Tl At 5G MEC Public Cloud g} [ 5GC User Plane 5 © % 5GC Control Plane HE e i 5G MEC on-premises 5G MEC on-premiseé', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 384, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5c64baa13d480a7216be19b09f6f47e2', 'text': 'Figure 6-27 Security Controls to Secure 5GC NFs and 5GC NF Traffic', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 384, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5ee2c9472152aba27b0f8994259b3276', 'text': 'Microsegmentation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 384, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd5f2cb143bd3263f6b999ebd69363700', 'text': 'Deployment of virtualized 5GC NFs require a new approach to network segmentation and access control. Microsegmentation is one of the primary methods by which this is achieved by following the principles of zero trust. The idea here is to ensure that specific policies can be applied to specific workloads without worrying about the nature of deployment of the 5GC NFs (VMs, containers, and so no) or the environment where the 5GC NFs are deployed (on-premises or public cloud), as shown in Figure 6-28.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 384, 'parent\_id': '5ee2c9472152aba27b0f8994259b3276', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '10f7eb210714ae496ba23ffc185c982f', 'text': '% Microsegmentation platform Jp— panadacan, gl i’ { — a] — T == Containerized & VM 5GC network 5GC Containers 5GC Containers 5GC network functions on BM on VM on Virtual machines functions on Public cloud', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 385, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'fcb94ca10a6e9805a6d3d863e12b18fe', 'text': 'Figure 6-28 Microsegmentation Applied to All 5GC Deployment Types', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 385, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4204caf57c59aeb7fce44f9402edb02b', 'text': 'To have an effective microsegmentation, its recommended to start with monitoring of the infrastructure and applications, understanding the behavior of various NFs, and then creating a baseline of behavior for all 5GC NFs and the relationship between the 5GC NFs and services like DNS, NTP, and so on. Once the data is collected and analyzed, you will have a better idea of how to segment them and isolate the workloads better. Various vendors have refined the algorithms to provide you with an automated segmentation. Microsegmentation in a 5GC container environment would need to include application context, such as a specific non-3GPP network function where integration or communication is required for specific use cases. This would allow you to reduce risk in case a workload has been compromised. Essentially, it means that a hacker who has breached a workload serving an application cannot move laterally to attack another application host. In this model, the hacker is isolated to the workload servicing the specific tier of the compromised host of the application. In real-life 5GC deployments, you would need to cater for virtual machines, containers on VMs, containers on BMs, and containerized 5GC network functions deployed on the cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 385, 'parent\_id': 'fcb94ca10a6e9805a6d3d863e12b18fe', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '61291b11c3c8cee673e0f64929b9a48a', 'text': 'The microsegmentation layer should be able to cater for providing isolation and applying segmentation policies for all modes of 5GC deployment. The microsegmentation layer should automatically tag security policies on all enforcement points in your 5G network, such as SDN, multivendor firewalls, or the workload level (virtual machine, bare metal, or container) by using', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 385, 'parent\_id': 'fcb94ca10a6e9805a6d3d863e12b18fe', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e7d537fec482aae0081783fb0f0ffcbd', 'text': 'software agents on servers (virtual machines, bare metal, or containers) to enforce a consistent, distributed zero-trust policy at scale. In some cases, there is no need for software agents because the microsegmentation policy can be enforced using the data processing unit (DPU) of your data center infrastructure. Although software agents are not required, closer integration between the microsegmentation solution and the DPU chipset vendor will be required.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 386, 'parent\_id': 'fcb94ca10a6e9805a6d3d863e12b18fe', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c99a393b33c16f0c1c137c23e64f9672', 'text': 'Application Service Mapping', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 386, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e3ba9a71a37222e70d0620e7b88cdc11', 'text': 'Application service mapping is sometimes referred to as application dependency mapping by vendors. Application dependency mapping is the process of figuring out which applications are dependent on what other applications and services. In 5G networks, application dependency mapping or application service mapping can be achieved by observing and collecting all interactions between applications and all systems and devices. Analytics is then used on this data to determine what 3GPP and non-3GPP 5G applications exist in your infrastructure and how these applications interact with other applications, systems, and devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 386, 'parent\_id': 'c99a393b33c16f0c1c137c23e64f9672', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '61b300acfe45389da1b25a8521100a66', 'text': 'Implementing application service mapping in your 5G network will provide you with the following key capabilities:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 386, 'parent\_id': 'c99a393b33c16f0c1c137c23e64f9672', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '55cc414da88c7634c904c07fcd6077c7', 'text': '• Understanding the services linked to the 5GC workloads, including 5G MEC applications. Figure 6-29 illustrates an example that shows the dependencies and services linked to an MEC application client.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 386, 'parent\_id': 'c99a393b33c16f0c1c137c23e64f9672', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '66c39d1c87040237428a62ff2bb90004', 'text': 'Appln Server “—r mySQL DB -~ 5G MEC 5G MEC Client Server Appln Server ) Cache “—> — redis = 4] — Webserver “— tomcat DNS Server +“—> CoreDNS | — | —', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 386, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3144c03c05a7cc5b179f5111bee6039b', 'text': 'Figure 6-29 Example of Application Dependency Mapping for a 5G MEC Application', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 387, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bcb37c4082004fdbc04feb3aebb2a5c9', 'text': '• Discovering and mapping 5GC workloads such as 5GC 3GPP and non- 3GPP NFs across multiple environments—hardware, on-premises virtual deployment, and public cloud deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 387, 'parent\_id': '3144c03c05a7cc5b179f5111bee6039b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2e5b89b885136aa458797879576cbe59', 'text': '• Discovering all types of 5GC workloads, including monolith, virtual machines, containers on VMs, and containers on BMs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 387, 'parent\_id': '3144c03c05a7cc5b179f5111bee6039b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '34c01d1dd8210f50edf6b2462f5f4d17', 'text': '• Discovering dynamic workloads (such as 5GC UPF network functions) and creating a topology map for the most recent instantiated workload.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 387, 'parent\_id': '3144c03c05a7cc5b179f5111bee6039b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '02a571619a86e70b5ebe6995b0ad02fe', 'text': '• Verifying the 5GC traffic flows against your customized segmentation policy for 5GC workloads.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 387, 'parent\_id': '3144c03c05a7cc5b179f5111bee6039b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '209770e5820139aba69f53d7127ae1c8', 'text': '• Indicating and creating alerts for any unauthorized traffic flows between 5GC workloads and between 5GC and non-5GC workloads.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 387, 'parent\_id': '3144c03c05a7cc5b179f5111bee6039b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '864cc43ae93fa9b6fd71c6845fd89078', 'text': '• Indicating and creating alerts for workloads not properly protected.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 387, 'parent\_id': '3144c03c05a7cc5b179f5111bee6039b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '68ddc61a36bc8284e7f6e024ffc1dcef', 'text': '• Simulating the 5GC workload impacts of adding or removing a service or security policy. An example would be showing you the impacts of adding a virtual firewall with a customized security policy between 5GC and non- 5GC workloads and the impacts it would have on the topology, such as breaking an existing active traffic flow that is required for certain 5G use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 387, 'parent\_id': '3144c03c05a7cc5b179f5111bee6039b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9fe364a5161437852d9367fdfba980eb', 'text': 'Application Performance Monitoring (APM)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 387, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b0b30c54e209e185c49659905e6aec22', 'text': 'In legacy technologies like 4G, key performance indicators (KPIs) such as availability rate, downtime, and so on were used to monitor the health of the infrastructure. In 5G, all the 5GC components are virtualized and deployed in different form factors and in different environments (on-premises/public cloud), so you need to look at performance monitoring a bit differently. The 5GC vendors will of course provide the KPIs related to subscribers, such as drop rates, inter-RAT and intra-RAT handover success rates, and so on, but you will still need deeper performance monitoring of the 5GC workload itself. You will need a solution to monitor the elastic 5G network function workloads, which are dynamic in nature, across your multiple virtual environments. This will be fulfilled by APM. The APM vendor you choose should provide you with the following capabilities for both 3GPP and non-3GPP workloads:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 387, 'parent\_id': '9fe364a5161437852d9367fdfba980eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '209edc26ba05deb3ec1b82ef67808718', 'text': '• Average response times of 5GC workloads: This is critical for ultra- reliable low-latency communication (URLLC) use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 388, 'parent\_id': '9fe364a5161437852d9367fdfba980eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0110239b39dc95b4c7edab096ac3d17c', 'text': '• Monitoring the uptime of the 5GC workloads: This is critical for multiple use cases, such as mitigating denial of service or interruptions for legitimate consumers accessing the applications or if you are providing certain applications to the 5G industry verticals and you need to maintain an SLA.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 388, 'parent\_id': '9fe364a5161437852d9367fdfba980eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '02f1a6c80d12749a95ecb8e6711be3ea', 'text': '• Monitoring the requests received per 5GC network function and detecting any anomalies: APM solutions need to create a baseline and a threshold for all your applications. Any change of behavior from the measured threshold can be indicated as an anomaly and lead to creating alerts.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 388, 'parent\_id': '9fe364a5161437852d9367fdfba980eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '87813681740a149198335b3fdff803cc', 'text': '• Continuous profiling of applications: Continuous monitoring the CPU usage, memory, and disk read/write speeds of the 5GC workload that are mapped to specific requests would enable you to determine if any requests are impacting the performance of 5GC workloads and give you code-level performance details. Figure 6-30 illustrates how this could be achieved.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 388, 'parent\_id': '9fe364a5161437852d9367fdfba980eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b7dce9fc554435486dd451b5366108c', 'text': '• API validation: This enables your 5GC development team to validate and test API calls and 5G network function workload impacts by mapping the performance impact for each API call. The changes can then be made by the development team before deploying them to production.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 388, 'parent\_id': '9fe364a5161437852d9367fdfba980eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c507d94358ba3bc145509a59accecfec', 'text': '• Monitoring user access: This provides you visibility into the users accessing the 5GC workloads deployed in your infrastructure, such as MEC applications deployed across multiple virtual environments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 388, 'parent\_id': '9fe364a5161437852d9367fdfba980eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '31d1022ad86e4642a84efd92d6a2a6cc', 'text': '• Openness and third-party integration: The APM you choose should also provide or allow you to integrate with the vulnerability detection system to ensure that the untested libraries with vulnerabilities are detected and flagged during the development stage before being moved to production.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 388, 'parent\_id': '9fe364a5161437852d9367fdfba980eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '7c7dc66f190eeda224e2a74781c228b5', 'text': 'Threat Policy defined Intel ML Al for Application User context and activity v RER Cloud 5GC Application Real-time analysis of application performance (rmtmn] oo ) To Application Policy activity and tracesi enforcement layer [ 7 - To Vulnerability detection A M User 00 and mitigation solutions 7 5G MEC Public Cloud ./// On-premises 5GC User \\/ workload activity A | and traces .// \\\\ a 5 User » [ ] ™~ % L 1 AT e T 5G MEC on-premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 389, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '69f13f34e92d5c9eb0152ff1f56bc125', 'text': 'Figure 6-30 Application Performance Monitoring for 5GC CNF', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 389, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'abd59d7df1535bda6ebce5312b080d39', 'text': 'Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 389, 'parent\_id': '69f13f34e92d5c9eb0152ff1f56bc125', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'fe75a2b99b3ae511791a8618f2b40284', 'text': 'Application Policy Enforcement', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 389, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e047c47aaf7067b4ee0b7d31894ac6b0', 'text': 'Traditionally you would enforce the policies for proprietary hardware using a firewall appliance. 5GC NFs being dynamic assets that can scale in and out depending on the traffic and use case requirements would need a smarter enforcement mechanism. 5GC NF application policy enforcement would need to stick to the 5GC NFs wherever they are deployed. This requires you to look beyond fixed network enforcement points. To enable the evolution of policy enforcement, you need the aforementioned layers of microsegmentation, application-to-service mapping, and application performance monitoring. Once you have implemented all these layers, the next step is to enforce the policies to the application/5GC NFs. The security policy for runtime could be, for example, what workloads can be deployed in what clusters and the connection rules that determine what connections can be set up between workloads. These connections need to be set at the workload level and not at the IP address or port level, which is usually done in firewalls, as shown in Figure 6-31. It could also contain deployment rules that control which workloads can be deployed in which environments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 389, 'parent\_id': 'fe75a2b99b3ae511791a8618f2b40284', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5abee1558e75e270de5a67e02fc7e3c5', 'text': 'Legacy method of Policy Enforcement Policy Enforcement for 5GC virtual deployments Policies enforced by firewalls Policies applied to Allow / Deny ‘ workloads directly IP address e instead of firewalls Ports etc == == Datacenter Server == == VMs, Containers > zwprietaw Pwpnelary Eroprietary on VMs / BM ssenrle- Lsow == Data Center Data Center Server Server', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 390, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2bcceb985aa9a65c50c3ba6485a1373c', 'text': 'Figure 6-31 Policy Enforcement at 5GC NF Level', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 390, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5abb5e1602fbcfd14dd0ff19d1550001', 'text': 'As illustrated in Figure 6-31, the policy enforcement could be done directly to 5GC network functions instead of the firewall using the orchestration system. Policies could be pre-fed into the orchestration system, such as pod security policies in Kubernetes, which is a cluster-level resource that specifies security aspects for the pod. The fine-grained policies could also be enforced by agents that can be installed by the policy enforcement solution on the VM, bare metal, container host, Linux, and so on. These sensors/agents would collect data from the workload (including process data, software package details, and so on) and inter-5GC NF communication and send it to the policy enforcement solution. This allows the policy to be attached to the 5GC NF and would be enforced wherever it is deployed, as illustrated in Figure 6-32.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 390, 'parent\_id': '2bcceb985aa9a65c50c3ba6485a1373c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f4df3d20500d7365d37af335aa8cdd39', 'text': '“Sticky” workload policy moves along with the 5GC workload [ -] 5G MEC Public Cloud il 5G MEC Public Cloud L] (] Migration of 5GC workload from on-premises to public cloud 5G MEC on-premises 5G MEC on-premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 391, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2f93b6716d021a993d6fd572ffe29955', 'text': 'Figure 6-32 Policy Stickiness Due to Policy Being Applied at NF Level', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 391, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd456402564f07514601fd66ef539bf29', 'text': 'Figure 6-32 illustrates the recommended method of policy enforcement, which is linked to the 5GC NF or application rather than based on the traditional method of segmentation based on IP address, port, and so on. The traditional network layer segmentation method will not be efficient for you because it cannot provide a granular security policy for mapping applications to users. There are solutions available today that enable you to have security policies based on the workloads.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 391, 'parent\_id': '2f93b6716d021a993d6fd572ffe29955', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '477a1a69d91e37ce5d3d90a530effd4d', 'text': 'These solutions, with both software agents and agentless options, allow you to scan container images and enforce policies as part of Continuous Integration and Continuous Delivery (CI/CD) workflows, continuously monitor code in repositories and registries, and secure both managed and unmanaged runtime environments. Some of these solutions also leverage the Istio service mesh for protecting network communications, multicluster communications, and secure communications with external resources as well as enforcing segmentation and workload isolation based on Layer 7 protocols mitigating pod communication with service mesh controls. These solutions also integrate with remote access virtual private network (RA-VPN) clients and Network Access Control (NAC)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 391, 'parent\_id': '2f93b6716d021a993d6fd572ffe29955', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e783f8a090a71b875803b1e257d838b2', 'text': 'for users and devices to bring user and endpoint context into the segmentation policy. This helps you to define granular policies to restrict application access based on the user, user group, user location, or other user-related attributes, as compared to enforcement of security policy based on just IP addresses and ports provided by traditional firewalls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 392, 'parent\_id': '2f93b6716d021a993d6fd572ffe29955', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '044e16cd9e3cc0f0c47d816dc3614ff9', 'text': 'Securing 5GC NF Orchestration and Access Controls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 392, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '588125a94806d5672beaf48a278c0566', 'text': 'Although you will have both VM and container deployments for 5GC NFs, a majority of the 5GC deployments would be based on containers (containers on VMs and containers on BM).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 392, 'parent\_id': '044e16cd9e3cc0f0c47d816dc3614ff9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '68368119067a10064465bd4c403c62b6', 'text': 'You will also need the deployments to be automated, scalable, maintain the state for the number of 5GC NFs, and provide secure networking for the containers. This should be catered for by the container orchestration solutions you choose. Due to the criticality of the orchestration function, it should support the security capabilities described in the sections that follow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 392, 'parent\_id': '044e16cd9e3cc0f0c47d816dc3614ff9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '33ab7a68864f05e47521e7bb84503f0c', 'text': 'Role-Based Access Control (RBAC)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 392, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ea4a84fe9e3e8f6f504319790218796c', 'text': 'RBAC will enable you to regulate access to the orchestration solution. The solution you choose should be able to work with on-premises and cloud- deployed access control systems. RBAC should also be used at the API access control layer to ensure you are authenticated before your requests are authorized. Kubernetes, which is a widely used orchestration system, authorizes API requests using the API server. It evaluates all of the request’s attributes against all policies and allows or denies the request; however, your deployment might have NFs that are not containers, and you need to ensure that RBAC is catered for by all the deployment nodes. Try to create policy templates that can be reused for a group of similar pods or applications; this will help you when you redeploy the applications or are deploying a similar application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 392, 'parent\_id': '33ab7a68864f05e47521e7bb84503f0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3bfbc243e06fd6e189c3c418e43b2a8f', 'text': 'Security Policies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 392, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '02d0045b411f494f26ee7becfdf05c48', 'text': 'For the containerized 5GC NFs orchestrated by well-known orchestration systems like Kubernetes, network policies are used to enforce segmentation policies. In Kubernetes, the 5GC NFs will be run in pods, which consists of', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 392, 'parent\_id': '3bfbc243e06fd6e189c3c418e43b2a8f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2991093002425ff201695d86ce18c5d2', 'text': 'one or more NF containers that are deployed together. Each pod is assigned an IP address and is routable with other pods. Network policies will determine the access permissions for those pods. In pragmatic deployments, however, you will have to manage large clusters with multiple orchestration platforms that contain several services developed by multiple teams. This includes third-party 5G MEC application services interacting with the 3GPP 5G NFs using the Network Exposure Function (NEF), which leads to challenges in having consistent security policies across different clusters. To solve this issue, you should implement multiple layers of security policy enforcement and look at deploying a service mesh, as discussed further in this section.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 393, 'parent\_id': '3bfbc243e06fd6e189c3c418e43b2a8f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '383528058955cb1131c0459983fbb716', 'text': 'The orchestration system you choose should offer the capacity or integration options with a solution that provides a security policy per workload within the pod, which is more effective, as illustrated in Figure 6-33. The chosen solution should also allow application-to-service mapping and visibility on 5GC NF-to- NF-level communication. The default policy should deny all requests so that you can select the right security policy for each and every workload or at least define a policy on a set of similar workloads. This can be planned well in advance, and methods such as the aforementioned Application Policy Enforcement will help you plan and enforce the policies across 5GC workloads.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 393, 'parent\_id': '3bfbc243e06fd6e189c3c418e43b2a8f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '4447be1a75b868be8503af444b50a9bf', 'text': 'Security policy [ Security Policy enforced at pod level —— e —————————] — —— Security Policy enforced at container level (/ Cluster node i container B / —\_——— e ——', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 393, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c60a20f3a985fbd3729f3abd4da3c43b', 'text': 'Figure 6-33 Security Policy Enforcement Levels', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 393, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'cd32fc2d83c83e53e82fa5f3c4d025eb', 'text': 'Secure Communication', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 394, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7c9eb6c7f275217b2fe4f9ddc7c227c8', 'text': 'One of the key challenges of managing virtual deployments of 5GC (specifically container-based NF deployments of 5GC), other than securing the container itself, is to understand how to properly secure and encrypt the traffic flow and communication between NFs. mTLS and TLS are recommended by 3GPP TS 33.501 to be used for inter-NF traffic flows. For 5GC NF-based deployments, vendors are aiming to provide TLS and mTLS options. The API calls from the container orchestration system to any internal or external container nodes should be protected by TLS, as illustrated in Figure 6-34.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 394, 'parent\_id': 'cd32fc2d83c83e53e82fa5f3c4d025eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ad2436c5a5a1027cec1abda8e23a9b02', 'text': 'Orchestration Engine VM Orchestrator Container Orchestrator API Server - TLS/mTLS TLS/mTLS TLS/mTLS i e e : Ol = [0 \\‘ 5GC VM deployment - 5GC Container deployment - 5GC VM & Container on premises on premises Public cloud deployment 5GC NF deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 394, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '64ff3574877dcb81c9af1a7684abb932', 'text': '5GC NF deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 394, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f91974ecfb94e7c00c4fc9e33eceff79', 'text': 'Figure 6-34 Secure Communication Between Orchestration and 5GC NFs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 394, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '642bbd1f5655a126dd4e032dee8c46bd', 'text': 'As illustrated in Figure 6-34, the communication between the orchestration system and the 5GC NFs should be encrypted using TLS/mTLS encryption mechanisms. For the VM orchestration, you would normally use a virtual network function manager (VNFM) and an orchestrator. For the container deployment, Kubernetes is widely used. It is recommended to use a dedicated PKI infrastructure for the 5GC components.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 394, 'parent\_id': 'f91974ecfb94e7c00c4fc9e33eceff79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5b9db6e03f8ab405f66de984946dfd6d', 'text': 'One of the other options could be to leverage a service mesh and use a method to add a layer of security capabilities, such as encryption and authentication,', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 394, 'parent\_id': 'f91974ecfb94e7c00c4fc9e33eceff79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bd8671d56440bfb7e941ea7d68e23997', 'text': 'between services inside your 5GC NF cluster and outside your 5GC NF cluster. A service mesh also provides more visibility for microservice interactions to the operations team, especially when observability and visualization of east- west cluster traffic are included as part of the service mesh solution. In deployments that have large clusters with multiple teams developing different 5G-related services, a service mesh will help you create a network encryption layer that allows all 5G-related services to communicate with each other securely. Basically, a service mesh consists of a control plane and data plane. In actual deployments, the data plane is typically implemented as a proxy such as Envoy that is run “out of process” as a sidecar component. The control plane caters for policy and configuration for the data planes running in the mesh. The control plane also allows telemetry collection, which can then be consumed by your network analytics and monitoring solution. In a service mesh, a sidecar agent is attached to each pod and provides communication between services by fine-tuning the set of ports and protocols that the proxy will accept when forwarding traffic to and from the workload. In addition, it is possible to restrict the set of services that the proxy can reach when forwarding outbound traffic from workload instances. Apart from providing secure communication,', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 395, 'parent\_id': 'f91974ecfb94e7c00c4fc9e33eceff79', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b661220a53677dbb151598e06f48d9b7', 'text': 'as', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 395, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e0936f27f85612de2b3fe186b36081f9', 'text': 'as', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 395, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eb97d3ffad7ea43180f83f7259a93c91', 'text': 'monitoring/tracing/logging, and they avoid service interruption because they allow you to write applications that limit the impact of failures, latency spikes, and other undesirable effects of network peculiarities. A service mesh could be designed using open source services like Istio. It is basically a mesh of Layer 7 proxies that aims to establish and maintain service-to-service connections, as shown in Figure 6-35.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 395, 'parent\_id': 'e0936f27f85612de2b3fe186b36081f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5eedc7b35a9b94ea1abddf178c8d0b49', 'text': "CSR CSR |8 (< 4—' Certificate Certificate and - / Private Key ( tl A <> mTLS ry (2) ;f ———————— ——— —— s ——— e ————— —\_————— e —— — — e e e s oy, e Pl", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 396, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'abe1c249c0a2c687780a0680dfb403c4', 'text': 'Figure 6-35 Secure Service to Service Communications in Service Mesh', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 396, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '260a1c0385dc6bb543e95de3311c9383', 'text': 'Secure Production Identity Framework for Everyone (SPIFFE) uses a form of X.509 certificate to provide a secure identification process to each and every workload. The framework, once completed, will provide an enhanced method of identification and will remove the need for passwords or API keys. Figure 6- 35 illustrates one of the methods for NF-to-NF/orchestration-to-NF authentication based on Istio’s service, which is explained as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 396, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '043e84aeaefa23c6fde7229fb750957d', 'text': '1. In a container-based 5GC NF deployment, all the 5GC NFs can be securely provisioned using an Istio service mesh with X.509 certificates. The Istio agent placed next to the Envoy proxy creates the private key and certificate signing request (CSR) toward the CA. The Istio service mesh uses Remote Procedure Call (gRPC), which is a protocol built on HTTP/2, to take the CSR. The CA in the Istio daemon (istiod) validates the CSR. Once the CSR', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 396, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd7f60f399a0a6e9627ed42d3657eab32', 'text': 'is successfully validated, the CA signs the CSR to generate the certificate. When the 5GC NF is started, the Envoy proxy will request the certificate and key from the Istio agent using the Envoy Secret Discovery Service (SDS) API. The Istio agent then sends the certificate received from istiod and the private key to Envoy using the Envoy SDS API. The workload certificate is then continuously monitored by the Istio agent.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 397, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '25f88251c66dd2c09e5f97e74801282b', 'text': '2. NF-to-NF security in Figure 6-35 is provided by Envoy proxies, which enable tunneling of traffic between 5GC NF 1 and 5GC NF 2, and is secured using mTLS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 397, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '06e2e0ff80def119cb0a0e847dccc611', 'text': '3. When the client-side Envoy starts a mutual TLS handshake with the server- side Envoy, the client-side Envoy performs a secure naming check to verify that the service account presented in the server certificate is authorized to run the NF service.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 397, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1a0cb2a5032d1b67bc4bc01001af2efa', 'text': 'Secure Access Control Based on Zero-Trust Principles', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 397, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e3cdbad0024c741432b2d48029ea35f6', 'text': 'While you’re designing the access control for the virtualized 5GC NF deployment, it is important to follow the zero-trust principles. This would ensure that each and every request has to go through multiple security controls, which reduces the risk of unauthorized access to 5GC NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 397, 'parent\_id': '1a0cb2a5032d1b67bc4bc01001af2efa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fb0da5a3beddfca446158203abe836f0', 'text': 'For the communication between the NFs, if you don’t use the Service Communication Proxy or any network security controls, it is recommended to have security controls that can cater for authentication, authorization, and validation as well as compliancy of the inter-NF API calls, as shown in Figure 6-36.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 397, 'parent\_id': '1a0cb2a5032d1b67bc4bc01001af2efa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '430769344730edb2fbc524c682890712', 'text': '] 3rd party secrets management/ | ( Encrypted Key management 5GC NF " Anti-DoS / Anti- store / authorization attributes Templates ) | L DD?S attributes T 5GC NF 1 1 3 v 5GC NF 1 Validation & (e > <P Compliancy " Cloud /on - — — e s e s S e e s i s s e s i s Cloud / on premises premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 397, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '22339360f3b3e1dce1cc231318c37c5d', 'text': 'Figure 6-36 Access Control for Inter-NF API Calls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 397, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c425c17232627c6fd274c151939e13da', 'text': 'The key features of the recommended security controls illustrated in Figure 6- 36 for 5GC NFs can be deployed as a part of the API GW/WAF solution or can be deployed separately, as detailed in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 398, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b0146dcc7d9db5fd07a4fc1edae1979c', 'text': '1. In the initial deployment of 5GC NFs—be it based on virtual machines or containers—the authentication would be based on a TLS/mTLS mechanism, as that is the method most of the 5GC vendors are focused on today. But once you have a widely deployed multivendor environment in a couple of years’ time, it would be important to have on-demand ephemeral secrets and access permissions to ensure that all the 5GC NFs, including dependent services like orchestration, are secured using zero-trust principles. This can be achieved using a secrets management solution that is provided today by multiple vendors and integrating that with your authentication management/authentication solution. The 5GC vendors you choose today should at least have a plan—not necessarily a roadmap, as many product teams would not provide their future product “secrets”—to ensure that the 5GC NF authentication can be performed by any third-party authentication/secret management solution you choose. This is particularly important for 5GC NFs that are deployed external to your DC. While choosing the vendor for secrets management, it is recommended to validate the encryption for data at rest and authorization capabilities of the provided solution. These aforementioned controls will bring a truly robust authentication strategy to your virtual 5GC environment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 398, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '53dadd025f6263d625f670db1adcea44', 'text': '2. The authorization capabilities should also be capable of integrating with the third-party secrets management solution. You should also be capable of integrating the authorization subsystems with the third-party authorization solution to provide enhanced capabilities such as centralized authorization for all API calls originating outside your network toward your internal 5GC NFs. As these API calls could be from your 5GC NFs, secure exposure NFs like NEF might be bypassed; this makes the integration of the authorization controls to the external third-party secrets and authorization management very important in hybrid 5GC deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 398, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ae57327866bc749fed8dd6c771c0522a', 'text': '3. Once the API calls are authenticated and authorized, they should be inspected for any anomalies or any invalid attributes. It is important to have the API validation at both the client side and server side. Many of the API validations today are server side due to developers not understanding the implications of improper API security design. This topic is explained in more detail in the “Secure API” section of Chapter 5.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 398, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f4d6e8a20219a103babfbcbf43fe735e', 'text': 'For seamless deployment, operations, and maintenance of virtualized 5GC NFs, the security design following the zero-trust principles, as illustrated in Figure 6-37, is recommended to be deployed to mitigate any risks due to unauthorized users accessing the 5GC NF environments. The key components of this design are the integration of the authentication and the authorization controls with the third-party Identity and Access Management (IAM), secrets management, and encryption key management (EKM) solutions with the multifactor authentication (MFA) solution, which is then integrated with application policy management, which includes the application-to-user mapping and application policy enforcement.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 399, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a45b9290cbad90d4af956604715cd5d4', 'text': 'e MFA \\ \' Application Policy 3" party Identity & Access Anti-DDoS / Anti-DoS Management secrets management/ Management altributes Encrypted Key management store / A authorization attributes 5 [ Validation & a 4—\_”7 Authentication 4—}‘ Authorization k—N Compliancy - 5GC NF User | S ——', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 399, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c6f55898704c72f7787b1253528e3776', 'text': 'Figure 6-37 Access Control for Users and User Devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 399, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bdf8d243f7f9156381f6bd4ce716ccb9', 'text': 'The security design illustrated in the Figure 6-37 is further explained as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 399, 'parent\_id': 'c6f55898704c72f7787b1253528e3776', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '422faed7a3def1dff5cb8f1325d12805', 'text': '1. Access control for 5GC users should be carefully planned to reduce any attack surfaces due to unauthorized access and privileged mode escalations. The multivendor 5GC NF deployment in hybrid virtualized environments should have centralized authentication for users accessing the 5GC NFs. The authentication solution should be able to provide multiple authentication methods such as JSON Web Tokens (JWT), Open ID Connect (OIDC), LDAP, RADIUS, and so on. Adoption of containerized 5GC will see many different options of how the policy is attached to the user. This is because', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 399, 'parent\_id': 'c6f55898704c72f7787b1253528e3776', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ca3d7ff57f74efa1df78aa260570db51', 'text': 'there are many standards allowing more compact and efficient methods of securely transmitting information between a client and a server using URL, POST attributes, or an HTTP header that are self-contained; there needs to be less to and from queries. One such method is JWT. When a user successfully logs in to the identity authentication server, it responds with JWT, which consists of what routes, resources, and protected services or 5GC NFs the user can access. This method is quite useful in API calls, which the user will have to use to access the 5GC NFs for any configuration or operational reasons. You should ensure that the 5GC vendor’s RBAC functions can integrate with the third-party IAM and secrets management solution. The MFA solution will enable establishing trust of the user and device by establishing user and device identity, checking the device posture and vulnerabilities, and ensuring access only if the device meets certain preset minimum criteria for access. All these security controls will provide a robust security posture for users accessing the 5GC NFs and allow you to future-proof your 5GC user access control mechanism.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 400, 'parent\_id': 'c6f55898704c72f7787b1253528e3776', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36d4e0e9676ba8fcd61adf96a6dfea24', 'text': '2. Application-to-user mapping (explained in detail in the section “Application Performance Monitoring” in this chapter) will enable you to further enhance the user-to-application authorization policies by providing the visibility of any users violating the application-to-user mapping. For example, if User A is mapped to 5GC NF 1 only and tries accessing 5GC NF 2, an alert should be created and should be able to be integrated with your existing logging and monitoring solution.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 400, 'parent\_id': 'c6f55898704c72f7787b1253528e3776', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f4d52e28e01f7ba3268d118b40029dea', 'text': '3. Once the user and device are authenticated and authorized, they should be validated for any unallowed URL or POST attributes and should undergo rate-limiting checks to prevent distributed denial-of-service (DDoS) or denial-of-service (DoS) attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 400, 'parent\_id': 'c6f55898704c72f7787b1253528e3776', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ef95e518fbf7e033f2bd9ecd74a3de02', 'text': 'Securing 5GC CNF in Roaming Scenarios', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 400, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e62ae15dc41b7da084f8461ca7075fd', 'text': 'Apart from the internal traffic flow in 5GC between the 3GPP and non-3GPP 5G network functions, the virtual 5GC deployments need to be secured against threats from external connections, such as roaming partners. Figure 6-38 illustrates the security controls for different 5G NSA and SA interfaces during a roaming scenario. In a pragmatic scenario, you will have 4G and 5G networks co-existing with each other. While you’re considering roaming interface, remember that a majority of your roaming partners for the next 2 to 3 years will still be based on 4G or 5G NSA deployments, which will require', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 400, 'parent\_id': 'ef95e518fbf7e033f2bd9ecd74a3de02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '32c3d1a5ff599bcae66f6db82b61d36b', 'text': 'Diameter and GTP-C protection for the control plane and GTP-U protection for the user plane.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 401, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '6a16cbf5f0cb9fa5eb9ef5c0ff16ceac', 'text': '‘E HSS + UDM PGW\_C + SMF \_ N7 hPCF VPLMN Séa $8\_C N16 PGW\_U + UPF N9 N8 N24 S8 U Control Plane FW SGW UPF VvPCF MME AMF N11 N15 N26 HPLMN S1-U S1-C N3 N2 (<A>) ((A)) eNB gNB', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 401, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'beff596f1a83bb5311d42d9c6d3feaae', 'text': 'Figure 6-38 Securing 5GC NSA and SA Roaming Scenario', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 401, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ee117e5c8fd332f5bf134a5fb65fa7f4', 'text': 'As shown in Figure 6-38, if your roaming partner is using a 5G NSA/4G deployment, control plane firewalls such as Diameter firewalls and GTP-C firewalls can be used to secure the roaming interfaces. For 5G roaming scenarios, the legacy protocols on the control plane, such as Diameter and GTP-C, have been replaced by APIs and a new NF called Security Edge Protection Proxy (SEPP), which is defined to secure the API communication between the home network and visitor 5G network. The SEPP function is defined by 3GPP to enable secure roaming interconnect between 5G networks. SEPP protects the control plane by performing mutual authentication and negotiation of the cipher suites. It also handles the key management aspects that include setting up the required cryptographic keys needed for securing messages between the home PLMN (HPLMN) SEPP and the visitor PLMN (VPLMN) SEPP apart from performing topology hiding by limiting the internal topology visible to the external roaming partners. As compared to the 4G roaming interconnect method, the SEPP function in 5G allows simpler', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 401, 'parent\_id': 'beff596f1a83bb5311d42d9c6d3feaae', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a07cbe78a968f291b3519881e9224ef3', 'text': 'configurations required to secure the roaming control plane. Figure 6-39 illustrates a simplified view of the SEPP function.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 402, 'parent\_id': 'beff596f1a83bb5311d42d9c6d3feaae', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd201ab3aceeccbd0bfbb0066ac31de2b', 'text': '4G 5G Standard API settings and simpler configurations !! HPLMN e I | VPLMN 5G Packet 5G SEPP 3GPP Core functions = - ((A)) 5G Radio Node 4G Radio Node', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 402, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7d366ca0992883920c91e2360b45cc8a', 'text': 'Figure 6-39 Simplified View of 5GC SEPP Network Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 402, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '46ee12a3aadf1ad6afb348a8e2572835', 'text': 'The SEPP function, as illustrated in Figure 6-39, secures the 5GC NF function from roaming threats by validating requests from 5G roaming entities. For securing the user plane communications, the 5G user plane function uses the Inter-PLMN UP Security (IPUPS), which enforces GTP-U security on the N9 interface between the UPFs of the visitor and home PLMNs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 402, 'parent\_id': '7d366ca0992883920c91e2360b45cc8a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3bb0bcfcad7262aab9347dec3082d5d3', 'text': 'Securing the Host OS and Hardware', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 402, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eec3ea235ebc89bd45f33170ee05c93c', 'text': 'The security of the hardware and software on which the 5G NFs would be deployed is very important for the overall security of the 5GC CNFs. Here are some key security controls and best practices related to securing the host OS and hardware for 5GC CNF deployments:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 402, 'parent\_id': '3bb0bcfcad7262aab9347dec3082d5d3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67106a6f7891c63cabb1db35a7e012d7', 'text': '• The host hardware for containerized deployment should be hardened as covered in detail in Chapter 5 in the section, “Hardening Hardware and', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 402, 'parent\_id': '3bb0bcfcad7262aab9347dec3082d5d3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c3b5dc898e6c17ed9161369cef9be626', 'text': 'Software.” The hardware should have the hardware root of trust using Trusted Platform Module (TPM) and Trust Anchor modules (TAMs). Host hardware should also support Unified Extensible Firmware Interface (UEFI). Methods such as UEFI secure boot detect tampering with boot loaders, operating system files, and unauthorized ROM by validating their digital signatures. This would help you verify if the code launched by the firmware is trusted or not, and any detections are blocked by running before they can infect the system.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 403, 'parent\_id': '3bb0bcfcad7262aab9347dec3082d5d3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4a44677c987bc7c338005209422071e7', 'text': '• It is recommended to validate the components for base OS and functionality, which is less of an issue for container-based 5GC NFs because most of the dependencies are packaged within the container. For any VMs being deployed, having the validation of the base OS and functionality is a critical step.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 403, 'parent\_id': '3bb0bcfcad7262aab9347dec3082d5d3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2c8cc865fc7a955102782fc70bced1ed', 'text': '• The dependencies on the host OS for the deployed 5GC NFs should be kept to a minimum. This is one of the key reasons why many vendors and service providers are aiming for container deployment for 5GC NFs. When you deploy a containerized 5GC NF, the dependency on the host is bare minimum, as most of the dependencies are packaged within the container itself. This brings in a lot of flexibility to deploy the 5GC NF wherever you want (on-premises or cloud). This brings in the need to have visibility and perform auditing on the guest OS for both VM and container 5GC deployments, which includes monitoring the resources being utilized and consumed by the 5GC NFs as shown in Figure 6-40.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 403, 'parent\_id': '3bb0bcfcad7262aab9347dec3082d5d3', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'cd224fb5cc4c41b549877cdf1d445cb9', 'text': "A CPU/ Memory [ Ill Public cloud logs, metrics with per 5GC ~— 5GC NFs » container / VM application insights on CPU and memory utilization Monitoring of resource utilization per 5GC NF per deployment type VM & Container Public (VM / Container) cloud deployment On-prem logs, metrics with per 5GC container / VM resource utilization | St e e S AT Enln o it T '\\ Data collection sensors / VM deployment - agents for OS level resource Container deployment - utilization data collection on premises on premises", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 404, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'bad664ce38b6f25e088449852612f8a6', 'text': 'Figure 6-40 Monitoring System for Host OS and HW', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 404, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '65930deeddeffe87b65f4c7a12b58ce8', 'text': '• It is recommended to keep the host OS current with security updates and any other component updates recommended by the vendor providing you with 5GC NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 404, 'parent\_id': 'bad664ce38b6f25e088449852612f8a6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c4462d21eca97fea714778cd32b27115', 'text': '• When 5GC NFs are deployed on VMs, hypervisors provide isolation and allocate resources such as CPU, memory, and storage to the guest OSs. This ensures that the guest OSs do not overlap on each other’s resources and mitigates the risk of DoS attacks caused by excess resource consumption by malicious code in a guest OS deployed in the same server/hypervisor. In real-life deployments, however, virtual machine deployments use guest tools, wherein the guest OS can access files, directories, and so on, on the other guest OS, or sometimes even the host OS. This could be used as an attack vector. The deployment of any such guest tools should be avoided if VMs are used for 5GC NF deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 404, 'parent\_id': 'bad664ce38b6f25e088449852612f8a6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b26c8165b73b956468350c2f7210885', 'text': '• Configure control groups (cgroups) to limit and isolate the resource usage for a group of processes. This will ensure that containers on the same host do not impact the performance of each other. Specifically, for this purpose, it is recommended to have the critical 5GC NFs placed on their own dedicated host so that the host can be secured specifically for the services offered by the critical 5GC NFs and so that an attack on any other', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 404, 'parent\_id': 'bad664ce38b6f25e088449852612f8a6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b0de854bb3d7a5ff21cc6ac4675bdc7', 'text': 'service would not impact the critical services. This strategy should be applied to any format of virtualization (VMs/containers).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 405, 'parent\_id': 'bad664ce38b6f25e088449852612f8a6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a975e045df1e26431eea9a7ea7ac73d5', 'text': 'Real Scenario Case Study: Virtualized 5GC Threats and Mitigation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 405, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '687af3da44dde5a0c84edf15d5224814', 'text': 'This section focuses on multiple attack surfaces on virtualized 5GC environments and discusses methods to mitigate the mentioned attacks. At the time of writing this book, 5G was not yet widely deployed, and the scenarios mentioned in this section are based on discussions with customers and experiences with lab and pilot deployments. Figure 6-41 illustrates the virtualized 5GC environment being considered for the case study.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 405, 'parent\_id': 'a975e045df1e26431eea9a7ea7ac73d5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f17e4b6bb0c1ddaf12099e13c0ea4f87', 'text': 'UPF MEC Application (5GC 3GPP NF) (5GC non-3GPP NF) < a 0 O | U.e S r < 4 MEC application API (to 5GC NFs (3GPP & non-3GPP) Non-AP! traffic (Internet traffic MEC - Public cloud & Internet / Roaming etc) DIA (Direct Internet AP Access) v ! AMF, SMF, NEF.. | > UPF MEC Application (5GC 3GPP NF) Billing (5GC 3GPP NF) (5GC non-3GPP NF) Transport over P Transport to > < Public network QHQH\_ o= DED =E = = = MEC on-premises Centralized 5GC on-premises deployment deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 405, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '90dd13e27b51c195483d62ad66773215', 'text': 'Figure 6-41 5GC Deployment Example for the Case Study', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 405, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c17de40a257c2f3bbe26a7cd23c2024d', 'text': 'As shown in Figure 6-41, the 5GC NFs are deployed both on premises and on the public cloud. The architecture for this deployment is explained in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 405, 'parent\_id': '90dd13e27b51c195483d62ad66773215', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '121a21d4e50f87c0d59d8d5120d130a4', 'text': '• The on-premises MEC DC has a 5GC 3GPP NF called intermediate UPF (I-UPF), which redirects the traffic flows to the designated UPF in the public cloud. I-UPF acts as a classifier that redirects the flows using traffic-matching filters. N9 is the reference point/interface between I-UPF and UPF session anchor. This design is reduces the latency and will help', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 405, 'parent\_id': '90dd13e27b51c195483d62ad66773215', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3606a6eceb12c172e89b4ee1afc2cdfa', 'text': 'you to validate the design and performance for ultra-reliable low-latency communication (URLLC) use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 406, 'parent\_id': '90dd13e27b51c195483d62ad66773215', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '73a75998feaf37c6067fc6989b992785', 'text': '• The MEC application is a third-party non-3GPP application that is deployed on the same DC where the I-UPF is deployed. It is located in the edge DC to terminate MEC application-related queries from IoT devices and sessions that are redirected from the I-UPF 5GC NF.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 406, 'parent\_id': '90dd13e27b51c195483d62ad66773215', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '01be26a4fa67d041dd999dcbbdf8736f', 'text': '• The MEC application and the I-UPF were deployed on the same server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 406, 'parent\_id': '90dd13e27b51c195483d62ad66773215', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'de56e381790681a6b92a5f7094009733', 'text': '• The MEC DC provides API external/northbound interfaces for orchestration and API calls between MEC applications. Non-API interfaces are provided to allow Direct Internet Access (DIA) for use cases that require Internet access from the MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 406, 'parent\_id': '90dd13e27b51c195483d62ad66773215', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dfb975f38240d6fe981b8f06d5676ab8', 'text': '• MEC layer using public cloud deployment is also considered to enable deployment of UPF and third-party MEC applications, similar to the on- premises MEC, with the only exception of I-UPF, which is dedicated in the on-premises MEC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 406, 'parent\_id': '90dd13e27b51c195483d62ad66773215', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5b8d510f938cb2e48a05f95672609d33', 'text': '• The centralized 5GC on-premises DC hosts the 5GC control plane 3GPP NFs such as AMF, SMF, PCF, and so on, 5GC user plane NFs such as UPF for non-URLLC use cases, and non-3GPP NFs such as dedicated third-party billing functions from vendors providing a telecom billing infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 406, 'parent\_id': '90dd13e27b51c195483d62ad66773215', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3162c0ad6cff042e2adc43706346f755', 'text': '• The transport infrastructure between the MEC and centralized 5GC deployment carry traffic between the 5G 3GPP NFs such as N9 (I-UPF < > UPF), N2 (gNB < > AMF), and N4 (I-UPF < >SMF).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 406, 'parent\_id': '90dd13e27b51c195483d62ad66773215', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4cc7e086b1bd8accf1ac2393ba6d016d', 'text': '• The centralized DC hosting 5GC NFs also provides API interfaces toward the MEC and orchestration layers. The northbound API from the centralized DC enables integration between the 5GC control plane NF deployed in the centralized DC with the 5GC control plane NFs deployed in the public cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 406, 'parent\_id': '90dd13e27b51c195483d62ad66773215', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1290b5c652c163a8173b0140df7328fd', 'text': '• The user shown in the Figure 6-41 is allowed access to both the cloud- deployed and on-prem NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 406, 'parent\_id': '90dd13e27b51c195483d62ad66773215', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4095944688b2a1f961946fe43dc25449', 'text': 'Threats Case Study', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 406, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cd01912edeb66e7f6f1309cc9ad70ec5', 'text': 'This section takes you through the threat examples in the virtual 5GC environment illustrated in Figure 6-42.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 406, 'parent\_id': '4095944688b2a1f961946fe43dc25449', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '424cf5999709407ee0bbf7acc4cb97da', 'text': 'UPF MEC Application (5GC 3GPP NF) (5GC non-3GPP NF) O < MEC application API (to 5GC NFs Non-AP! traffic (Internet traffic MEC - Public cloud & Internet (SGPP& non-3GPP) Roamlng efc) DIA (Direct Internet AP 2 Access) UPF MEC Application AMF, SMF, NEF AM (5GC non-3GPP NF) (5GC 3GPP NF) Billing (5GC 3GPP NF) Transport over <« Transport to N gNB Public network = Centralized 5GC on-premises MEC on-premises deployment N i deployment [ User', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 407, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e5e9293610c091e9445b880590f76938', 'text': 'Figure 6-42 Threats Scenarios', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 407, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '68afcfae261e5d9c43709e643d1dc7f7', 'text': 'Figure 6-42 shows multiple attack vectors in the deployed 5GC network:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 407, 'parent\_id': 'e5e9293610c091e9445b880590f76938', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a7db48737e7c4ba971be36b799e75818', 'text': 'A. A single server is used to host both the 5GC NF and MEC application. This increases the risk for high-sensitivity workloads such as 5GC 3GPP UPF workloads being impacted due to lower security measures undertaken in the lower-sensitivity workloads such as MEC applications. MEC applications created by third-party developers usually don’t apply robust security policies, which leads to attack vectors such as unauthorized access to secure applications by using privilege escalations. In Figure 6-43, attackers use a weak API implementation on the MEC to gain access to the host OS. Once attackers gain access to the host OS and hardware (HW), they can access and exploit the 5GC 3GPP NFs and perform actions such as destroying the containerized 5GC NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 407, 'parent\_id': 'e5e9293610c091e9445b880590f76938', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ca0e793cb2252815ef86e7af66abea17', 'text': '‘ User / Attacker 5GC NF exploited due Improper API to vulnerabilities within the MEC Application implementation ST P — é 5GC 3GPP NF —> — [\_T\_] G] . MEC Application Lo E Host HW & OS Y S S S S — Attacker using the weak MEC application and escalating privilege to access Host OS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 408, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '54b876c9b746f15018c740a2f345bda3', 'text': 'Figure 6-43 5GC NF Impacted Due to Weak Security in MEC Application', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 408, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '53265f77305ac6bc9ef94d575cb1ebda', 'text': 'B. The MEC DC provides an API interface to enable inter-NF SBI-based communications that are prone to API vulnerabilities. The 5GC vendor provides 5GC NFs based on service-based architecture (SBA) implementing a service-based interface (SBI) that employs a RESTful API interface using HTTP/2. Secure implementation of API purely depends on service providers and vendors providing 5GC. Attackers can steal or modify such weakly protected data to conduct fraud, identity theft, or other crimes. Sensitive data might be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions. But the most seen issue during proof of concepts or during conversations with different customers is security misconfiguration. This is due to improper deployment methods such as detailed error messages with component details being sent to the user, using insecure default configurations, incomplete configurations, misconfigured HTTP headers and unpatched vulnerabilities, and improper security configurations related to rate limiting for API calls, as shown in Figure 6-44. Improper security configurations allow the attacker to do the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 408, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f20b38bc6d5a8240e553000dba661b5a', 'text': '• Understand the APIs being used internally', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 408, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1c4059e1c958daa74e7b25728d6af72e', 'text': '• Map the various services integrating with each other by gaining insight on NEF/SCP/NRF NFs, which opens up doors to attack chaining', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 409, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0a69a08607819265f9858199f6a70c8a', 'text': '• Gather the versions and types of applications and NFs being used', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 409, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bb75699332da088309c6c57cc33de177', 'text': '• Deny service to the 5GC system by forcing the system into a deadlock or an unhandled exception', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 409, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '020dae09bda14f8da481589bf3e18642', 'text': '(- An error occurred in line: 5 in the jsp file: /john/left.jsp MEC hosted in - Public cloud 2 R POST Error —\_— — e message L | v ( Py gy g gy, 1 3 l:lote: The full trace of the root cause is \\ available in Apache Tomcat /6.0.0 logs ey iy ey e 20 User / Attacker This message in the error informs the attacker that the application runs on Tomcat MEC hosted on-premises version 6.0.0. The attacker can use this information to attack the Apache Tomcat API web server', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 409, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '48dc0f998272dfdac5f2684c727a35d4', 'text': 'Figure 6-44 Security Misconfiguration Example', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 409, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fef888e0572a389e9bf4912c18151c1f', 'text': 'As illustrated in Figure 6-44, improper API security configurations such as passing more information in the error message to the API user would result in the user/attacker having information such as the API server being used and where the log is being stored. The attacker can then check the web server vendor’s website for security vulnerabilities and can attack the web server. In many instances, the security vulnerabilities in the web server are overlooked by the packet core team, as it is not a part of the main 5GC subsystem. This vulnerability, if left unpatched, would increase the risk for the virtual 5GC environment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 409, 'parent\_id': '48dc0f998272dfdac5f2684c727a35d4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e51bf2d976ea4ff14804e03ccbd5d628', 'text': 'C. Using cloud-native methodology to develop 5GC opens up an entirely new way of deploying 5GC NFs. This includes VM-based and container- based NFs that are constructed using open source and polyglot programs the developer is comfortable and efficient with. This new development of 5GC NFs also brings in new attack vectors due to vulnerabilities existing in the open source programs used in 5GC NFs. This vulnerability can be exploited by the attacker using API calls with escalated privileges to exfiltrate sensitive information or to change attributes within the NF to cause a DoS, as illustrated in Figure 6-45. As the 5GC CNF development is in its infancy, these threat surfaces are quite frequently found in the 5GC NFs from various vendors.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 410, 'parent\_id': '48dc0f998272dfdac5f2684c727a35d4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '75f608214ffc095a1b5994a868664069', 'text': 'UPF MEC Application Attacker exploiting the (5GC 3GPP NF) (5GC non-3GPP NF) vulnerabilities in open-source O components in 5GC NFs MEC - Public cloud & Internet t MEC application ) API (to 5GC NFs User / Attacker (3GPP & non-3GPP) +— 322 —> UPF MEC Application , SMF, NEF.. OAM (5GC 3GPP NF) (5GC non-3GPP NF) (5GC 3GPP NF) Billing < \_ Transport over ) Public network = = = fii = MEC on-premises Centralized 5GC on-premises deployment deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 410, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9b675c85607e4d3c6a3c06329089624b', 'text': 'Figure 6-45 Attacker Exploiting Weak Security in 5GC NFs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 410, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fc30973a9bdaafd71b1e5ca529294c42', 'text': 'D. One of the key risks in virtualized 5GC deployments is related to improper access control for users trying to access 5GC NFs and 5G related MEC applications. Due to the dynamic scale-in and scale-out nature of 5GC NFs, it is quite complex to maintain the user to application mapping using traditional segmentation methods such as network layer controls. The other key risk is the inconsistency of access management policies between multiple identity and management (IAM) solutions. The primary mode of access control provided by 5GC equipment and software', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 410, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c4bc2cca4c4068be3b980c42ed3181a5', 'text': 'vendors are based on role based access control (RBAC). This RBAC is then integrated with an identity and management (IAM) solution with customized policy for access control. Due to the nature of commercial offers from 5G vendors, majority of the vendors usually providers an option of its own IAM solution or partner IAM solution as a bundled offer. This leads to multiple IAM solutions with inconsistent policy implemented in your network, making the access control inefficient and inconsistent as shown in Figure 6-46.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 411, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'dc77d22be2fd926eb4b24b7dcbbd076e', 'text': '(] IAM - provided by public cloud provider 5 O ot e R L 5GC VM & Container a Public cloud deployment User E—— l.—b Multiple configuration points : Inconsistent user access configuration Complex to synchronize and T inefficient to maintain for real life virtual environments 1,, yu| = n @ n 5GC VM 5GC Container E e deployment - on deployment - on premises premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 411, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9efcfa31a871d9da14e895e2a1d39179', 'text': 'Figure 6-46 Improper Implementation of IAM for 5GC Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 411, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f0838938635f768900309054384735d7', 'text': 'Mitigation Examples', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 411, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e3eac1dac77a48c4e6f929e83a92a8f7', 'text': 'This section takes you through the techniques to mitigate the threats described under the “Threats Case Study” section based on the deployment illustrated in Figure 6-41. This section will be of particular interest to readers who are involved in a proof of concept or in early stages of virtualized 5GC deployments. Figure 6-47 illustrates the method used to deploy the virtualized 5GC 3GPP and non-3GPP NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 411, 'parent\_id': 'f0838938635f768900309054384735d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '584077821879029ace3d5c4ceb4052c6', 'text': 'To Internet To Internet for 3GPP and non-3GPP Separate Host OS & HW T MEC Application UPF MEC Application (5GC non-3GPP NF) (5GC 3GPP NF) l (5GC non-3GPP NF) (5GC 3GPP NF) l 00O fiid fiid [c=] Recommended practice of deploying virtual 5GC 3GPP & non-3GPP NF environments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 412, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bc004c4c1179a66092f7dbbbebce557c', 'text': 'Figure 6-47 Separation of Critical and Non-Critical 5GC Workloads', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 412, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd2f3f3b488862b85cb745ddd227ee40e', 'text': 'As shown in Figure 6-47, it is considered best practice to deploy the non-3GPP 5G NFs, such as MEC applications, in a separate NFVi infrastructure from the 5GC 3GPP NFs, specifically when the non-3GPP NFs are exposed to the Internet. In the containerized deployment of 5GC NFs, it is good to verify with the 5GC vendor if any data or state is stored on the host or if any application- level dependency is required to be provided by the host. Any dependency of a containerized 5GC NF toward the host OS and HW should be prevented or kept to a minimum. This will reduce the attack surface to a great extent, provide you with an easier way to identify any anomalies, and allow you to air- gap NFs that do not need exposure to the Internet. All the dependencies should be packaged within the 5GC NF image itself. 5GC vendors are working in this direction but are not yet there completely.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 412, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'text': 'Enhance Security Configurations and Handling or Error Messages/API Exceptions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 412, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8f96634989ca0d6f2ad9e038f1241096', 'text': '5GC NF deployment is based on SBA and uses API calls to communicate between the NFs and between the NFs and non-3GPP functions. To mitigate the risks due to improper error handling and exposing more information within the error message, the following steps should be taken by the 5GC vendor and service provider.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 412, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '182ad2cd6e7bfbf0b1c8d8047a0a0eab', 'text': 'Here are some key checks to be done by the 5GC vendor:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 412, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3c1627283c5aea7b02dbc0fdab9a0e6e', 'text': '• The testing team of the 5GC vendor should ensure that error messages don’t provide the user with extra information, such as the version and vendor type of the API web server being used in the infrastructure, as illustrated in Figure 6-44.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 413, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '35d9ac8113c6edfb9ab9bafee3e4767c', 'text': '• The testing process by the 5GC vendor should include checks for Top 10 OWASP vulnerabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 413, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ac6e4b86eaace6e20d5e854d1a383500', 'text': '• The test and validation team of the 5GC vendor should ensure that default and known files have been removed before moving the API server code to a production image that can be downloaded by customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 413, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5ba9a74c55b268b907ed58743a235732', 'text': '• The test and validation team of the 5GC vendor should ensure that debugging code or extensions have been removed before moving the API server code to a production image that can be downloaded by customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 413, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e8ee0a2d10660cc8dbc036693fc03c7b', 'text': '• Ensure that the logging mechanism of the API server is customizable and can be set by the customer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 413, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4954bd8e2672094aab492f3b802034ed', 'text': '• The testing team should validate the expected input type (JSON, XML, and so on).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 413, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5c774c17c8dc6bb6c09411206113fed2', 'text': 'Here are some key checks to be done by the service provider:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 413, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3e631257a3748025d4b2d4a7b70a6b0e', 'text': '• It is recommended that you understand the key points (east-west, north- south) of API calls within your deployment. This includes inter-NF SBI API calls, NF-to-third-party API calls, API calls to and from the orchestration solution, and API calls to and from the OAM solution. Having this understanding would allow you to map the weaker parts of your infrastructure that need security control enhancement.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 413, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '73c26216dc207b32d24e99092e7eb86c', 'text': '• Ensure that the default password for the API server is changed and updated.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 413, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a7fc4855fd5f72265e1b22871492999f', 'text': '• Ensure that the logging mechanism is secure and, if required, can be chosen to be encrypted at rest.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 413, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '54c9604b2709d362aed2335be1aa63d2', 'text': '• Ensure that the API server is configured to handle overloads and that you have options to rate-limit the API calls to prevent any DoS attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 413, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '105a490ca07326900ee421affad8eccb', 'text': '• Use an API GW/WAF for securing the external API calls and use TLS/mTLS to secure 5GC SBI traffic flow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 413, 'parent\_id': '3cb1ea97745e3d753dd393d7d9b457ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '81875d62f4bca89f5a9f7b04c6ce5326', 'text': 'Vulnerability Assessment and Patch Management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 413, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '55658e5e15264f277bc010134f56af9a', 'text': 'Figure 6-48 illustrates the mechanism to mitigate the vulnerabilities of the open source components used in the 5GC NFs. The security controls illustrated in Figure 6-48 and the best practices are explained in the list that follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 414, 'parent\_id': '81875d62f4bca89f5a9f7b04c6ce5326', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '049fd30e5c294643172c31c9383b5404', 'text': 'Coem )y (s ), Vulnerability Assessment and Patch Management A A ! UPF (5GC 3GPP NF) API (to 5GC NFs O MEC - Public MEC application (3GPP & non-3GPP) cloud & Internet A API <« UPF AMF, SMF, NEF.. MEC Application (5GC 3GPP NF) (5GC non-3GPP NF) — 5GC 3GPP NF) Biling Transport over, +——> > Public network == o — | (=T —] 0= Centralized 5GC on-premises MEC on-premises deployment deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 414, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '436db52dc813ba3c57c0cbf22eb5ee85', 'text': 'Figure 6-48 Vulnerability and Patch Management for 5GC NFs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 414, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3c922037b68b106b3ef918ec91d6cd31', 'text': '• Although the 5GC NFs are now based on open source components, some vendors are still planning to provide patched images a couple of times per year. Although this might be an increased number of patches of one to two times a year from previous deployment methods, it is not efficient enough. This is bound to improve once the 5GC vendors undergo more rigorous testing procedures and secure CI/CD procedures using a DevSecOps process where security is embedded into every stage of the software cycle, reducing the vulnerabilities and thereby reducing the patch cycles. Ideally, patches should be deployed as frequently as required, as soon as a vulnerability has been identified and patched open source software released. But in real-life scenarios, it would be good to have more', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 414, 'parent\_id': '436db52dc813ba3c57c0cbf22eb5ee85', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '80140055fcaca895fbe59ffaa7db6b33', 'text': 'frequently patched images with a possible frequency of once per month and then based on the severity of the exposed vulnerability. The reason a patching frequency of at least once per month needs to be checked is not for ensuring that each month the vendor has to release a patch, but to ensure that if there are multiple severities detected, the vendor has a process in place to provide expedited patched images that are signed and uploaded in a trusted registry for you to download and deploy.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 415, 'parent\_id': '436db52dc813ba3c57c0cbf22eb5ee85', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '120e33cfd566ee0c7447023b6786e15c', 'text': '• 5GC vendors should use semi-structured inputs while fuzz-testing the 5GC NFs to validate the input verifications done by the 5GC NF and check whether it throws any exceptions. If the fuzz testing is not being carried out on the 5GC NFs, it’s time that you start the fuzz testing for the 5GC NFs—at least the NEF and SCP NFs, which will be exposed to the Internet.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 415, 'parent\_id': '436db52dc813ba3c57c0cbf22eb5ee85', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '653f938cd11e31da9e142bcb5110e01b', 'text': '• The 5GC NFs you deploy should be capable of being integrated with a vulnerability solution that can cater for all modes of virtual deployments, such as virtual machines, containers on VMs, containers on BM, and virtual instances deployed on the public cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 415, 'parent\_id': '436db52dc813ba3c57c0cbf22eb5ee85', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fd582d2678068518e9933146e48d883f', 'text': '• The vulnerability assessment solution you choose should have integrations with the threat intelligence and Common Vulnerabilities and Exposures (CVE) database, which will enable you to identify the vulnerabilities in your entire virtual environment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 415, 'parent\_id': '436db52dc813ba3c57c0cbf22eb5ee85', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '14e8ad9cde1a3c40407bcfe94153369a', 'text': '• The vulnerability assessment solution should also allow you to mandate policies such as isolating web-facing workloads with a certain condition, such as having a CVE severity score of greater than 9 after giving the developer a certain period of notice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 415, 'parent\_id': '436db52dc813ba3c57c0cbf22eb5ee85', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6d7faf6dfcfe7a81a540ea9258a05a11', 'text': 'Granular Access Control Based on Zero-Trust Principles', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 415, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c0325bc2955ed402e97f8f0a252c17b8', 'text': 'Figure 6-49 illustrates the security controls and mechanisms to mitigate the risk of improper access control for the 5GC NFs. The list that follows explains this in more detail. This method can be used for access control for all CNFs in 5G deployments, including 5G RAN, core, third-party MEC applications, and orchestration functions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 415, 'parent\_id': '6d7faf6dfcfe7a81a540ea9258a05a11', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '2f3222b944306722f100138786c0f6c6', 'text': 'IAM 1 RBAC 1 IAM 2 RBAC 2 0 b Security admin Identity Provider Policies l User Policy: User 1 T -h Allow access: 5GC NF 1; 5GC NF 2 - —\_— User 1 ~————p| Authentication |—» Deny Access: 5GC NF 3, 5GC NF 5 <4 Post Authentication v v X X 5GCNF 1 5GC NF 2 5GC NF 3 5GC NF 4 D B Do O] On-premises or Cloud deployed', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 416, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '38d65ba00a426cec33c2ce24eb1603f7', 'text': 'Figure 6-49 Access Control Policy Deployment Example for Users Accessing 5GC NFs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 416, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1a3dc529c04d8a09c0a7089c4df9c22d', 'text': '1. The 5GC vendor you choose should allow the integration of their RBAC with an external authentication server. The authentication server you choose should be able to be integrated with multiple IAM solutions. This is actually one of the most overlooked issues in identity and access management for 5GC deployments. Many miss the fact that each 5GC vendor might have a preferred IAM vendor or an integrated IAM (part-IAM) solution for access control. If you choose around four to five different vendors only for the 5GC solution deployment, you will have an extra four to five IAM solutions to operate and maintain. We are seeing this in pilot deployments already, and the production systems will have the same issues. The primary point here is not about cost, as the IAM solutions can be deployed for a few thousand dollars/euros, but about efficient identity and access management for your end-to-end multivendor 5G solution, including the 5GC domain.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 416, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '724b1a7154ecf1eadebd45b34e996d4d', 'text': '2. The solution you choose for the IAM should provide you with the option of configuring custom policies for users and should be able to map users to applications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 417, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '53e497aaadd74ac2a74a73444c168589', 'text': '3. The authentication solution should be able to provide multiple authentication methods such as JSON Web Tokens (JWT), Open ID Connect (OIDC), LDAP, RADIUS, and so on. Using a method such as JWT, claims can be transferred between the user and authentication server. These claims are encoded as JSON objects, which are digitally signed using JSON Web Signature (JWS) and, if required, encrypted using JSON Web Encryption (JWE). Based on these claims, the user will have access (or not have access) to the 5G NFs. For example, the authentication solution can set a claim saying ‘isAdmin:true’ and issue it to the admin user trying to access the 5G NF or third-party MEC application to make configuration changes upon successfully logging in to the application. The admin user can now send this token in every consequent request to the authentication solution to prove their identity.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 417, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7220a0ad55973550342e82671cd3896a', 'text': 'This method can provide granular access control by ensuring mapping between users and applications, including the role of the user or application, to determine if the user can access and modify the configuration of the 5G NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 417, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1b3e17ebac72cf25491390729756a2ec', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 417, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7f7eb43e324ea3032f1aabd9cf6c099d', 'text': 'As discussed in this chapter, 5G brings the cloud-native approach to developing 5GC network functions using an open source software stack, deploying and maintaining the 5GC network functions dynamically enabling elasticity, optimizing the use of resources, improving overall agility, and bringing together a whole new software ecosystem that can integrate with your 5GC. It also brings in new threat surfaces not present in previous technologies, requiring a mindset change in the way you perceive security for packet core and ecosystems, depending on your packet core. The section “Threats in Virtualized 5G Packet Core Deployments” took you through the key threat surfaces in virtualized 5GC deployments, where different threat surfaces are explained in detail. The section “Securing Virtualized 5G Packet Core Deployments” then took you through the mitigation techniques in detail. You also saw the real-life scenarios where customers are concerned about the attack vectors and risks during the initial deployment of 5GC as well as some of the threats that have been seen in present deployment phases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 417, 'parent\_id': '1b3e17ebac72cf25491390729756a2ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '52a960b4fd8ffef51bf77cff4caf0893', 'text': 'Figure 6-50 illustrates multilayered security controls to secure virtualized 5GC deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 418, 'parent\_id': '1b3e17ebac72cf25491390729756a2ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c009784ae59d53b3bcb49e80128987a3', 'text': '= Roaming Partners 5GC CNFs deployed in Al public cloud & Internet CEEe > = = 5GC CNFs 5GC CNFs deployed in deployed in MEC Centralized DC Inbuilt HW & SW security layer Enhanced Access Control layer for NFs and Users Application protection & Policy enforcement Enhanced Visibility, Anomaly detection, Analytics & Monitoring AP security (AP Gateway, API Firewall) Security Gateway, NGFW, Advanced Anti -Malware & DDoS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 418, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '55a3245ab02ba8d66fb062797b1d5b25', 'text': 'Figure 6-50 Multilayered Security Controls to Secure Virtualized 5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 418, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '62490369239f8326a802e0baacf0d4ec', 'text': 'Figure 6-50 Multilayered Security Controls to Secure Virtualized 5GC Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 418, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '660d03898c05e70d6a9d02bd22895043', 'text': 'Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 418, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2c033ca4ceb8403c83e0604136b62d0', 'text': 'Figure 6-50 illustrates the key security controls needed to secure the various deployment modes of virtualized 5GC NFs. The security controls can be reused for other parts of the infrastructure but are mapped here specific to the 5GC so that the reader interested in only this section can identify the key multi-security layers required to protect the virtualized 5GC deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 418, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c8edcb5c48dc663ffa4de61209e1dd0c', 'text': 'The security layers required to secure virtualized 5GC deployments are summarized in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 418, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2e58ba907540c79a6f1862baa760f4fb', 'text': '• Built-in hardening: Ensure that the host OS and the firmware of the host HW are patched regularly to prevent attackers from exploiting the host OS for attacks based on privilege escalation or, in the case of HW, to narrow the possibilities of attacks based on side channel. It is recommended to use server manufacturer–supplied patch management and secure boot', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 418, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '18d8e9f7f469dd81ae71e7b14b756463', 'text': 'visibility solutions, which will help you to identity the patch history of the firmware and also alert you whenever a vulnerability is exposed and when the corresponding patch is made available by the vendor.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 419, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '81f68d58f88df095c589dcfa50ace95a', 'text': 'The 5GC deployment should follow the true immutable manner where critical data is not stored on the host OS. The containerized 5GC NFs should have all the necessary application dependencies within the container itself, making it truly stateless.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 419, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5b0b4e1602241d559cd96927c10e3509', 'text': 'The hardware should have the hardware root of trust using Trusted Platform Module (TPM) and Trust Anchor modules (TAMs). Host hardware should also support Unified Extensible Firmware Interface (UEFI). This will help you verify whether or not the code launched by the firmware is trusted, and any untrusted code executions are stopped before they can infect the system. The hardware vendor should be able to provide you with the supply chain security measures it has undertaken. This is very important if you plan to use the hardware for 5G use cases for critical verticals such as public utility and national security verticals.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 419, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '887a141f611a1e0fd579c0aa9657af81', 'text': '• Enhanced access control layer: Due to the flexible deployment nature of 5GC workloads and API being the mode of communication, access control needs to be carefully planned while deploying 5G CNFs. 5GC vendor should provide role-base access control (RBAC) capable of being integrated with third-party access management solutions which support secrets management and encrypted key management. Network administrators and teams from vendor or contractors who configure and maintain the multi-cloud deployed 5G NFs should be allowed access only after they go through Multi-Factor Authentication (MFA) process and after verification of devices used to configure the network. For containerized deployments of 5GC NFs, deployment of service mesh will enable the developers to focus only on securing the application they are developing. Service mesh options like Istio provides the underlying secure communication channel, and manages authentication, authorization, and encryption of service communication at scale.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 419, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ea9bca7c110b8239dd7a8caa1ec93024', 'text': '• Application protection: With the cloud-native deployment approach using CI/CD methods as well as options for deploying containerized instances from vendors, the whole security ecosystem around having network security first has now changed to having application first security, which means you will now think about securing applications and their dependencies first, be it 5GC 3GPP NFs (VMs/containers) or non-3GPP', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 419, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67fb415d415b40af1f653e8734afb7f7', 'text': '5GC NFs such as third-party MEC applications. Having a secure 3GPP 5GC NF starts with the vendor having robust CI/CD solutions to ensure any vulnerabilities are captured early in the development lifecycle and rechecked and audited again before the images are signed and uploaded into a container registry for customers to download and deploy.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 420, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b37917eb7f8574faff3ae5cfe234edce', 'text': 'You should deploy vulnerability scanning for all the virtualized 5GC components deployed in all types of virtual environments, such as on- premises and public cloud. You should plan to deploy solutions for vulnerability management that make use of artificial intelligence (AI) and machine learning (ML). The will improve efficiency and provide quicker time to detect (TTD). You will need to look at solutions that provide an application-level policy; in other words, not only network-level policy creation but container-level policies that can be mapped to users and other applications. Mechanisms like microsegmentation and providing sticky policy mappings between users and applications will have to be planned and implemented once your network starts to scale using multiple deployment models.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 420, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f614ddc4ccc9df092c2a002313d8167e', 'text': '• Enhanced visibility, anomaly detection, analytics, and monitoring: To mitigate risks related to poorly implemented security controls within third-party applications and any vulnerabilities within the 5G CNFs, it becomes very important to have an enhanced visibility layer. For this to happen in virtualized 5G CNF deployments, the 5G vendor should provide the integration options with external monitoring solutions. This will allow the service providers to have a centralized monitoring system for a multivendor 5G ecosystem.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 420, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0688505e82bc91bc8766d01efd3fcb95', 'text': 'You should also ensure that the 5G vendors allow integrations with external monitoring solutions, even if the 5G vendor provides its own vendor- specific inter-NF-monitoring capability. This is due to the fact that you will have multiple 5G vendors in your network due to the new open 5G ecosystem. You should also look at having enhanced visibility at the encrypted layer without having to decrypt the encrypted traffic. There are vendors today who provide these capabilities using AI and ML techniques.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 420, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3b325b8cd2719fa8257ee243c95eaf0a', 'text': '• API security: The starting point of having a secure API is the definition of the API itself, which should undergo robust testing to fill any gaps or identify any security misconfigurations. You should also have detailed API security layers to ensure the validation of API calls, verifying the API calls for any malformed requests or packets, ensuring that the API calls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 420, 'parent\_id': '62490369239f8326a802e0baacf0d4ec', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3e48e2b0dc8eb0066466f1c06d82e9ea', 'text': 'are authenticated, and ensuring that policies are applied to the API request using mechanisms such as JWT Tokens and ensuring that critical information is not passed on the users. Orchestration API calls should be checked to ensure they are valid orchestration API calls and that any critical attribute changes should have multilayered authentication before they are executed. Auditing of the entire API ecosystem (SBI as well as external API) should be carried out at least every 3 months, and the encrypted API calls should be continuously monitored for any anomalies without having to decrypt them.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 421, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '88b3c953fafd79b84641f80feeb09a69', 'text': '• SecGW, NGFW, advanced anti-malware, and DDoS security layer: The initial deployment of 5G CNFs is aimed at on-premises DC and limited deployment on the public cloud. 5G NFs being deployed in the public cloud requires integration with the on-premises 5GC NFs, which can be protected using encrypted API calls. Any non-API calls can be protected with IPsec by using a security gateway (SecGW). The network layer segmentation of the NFs and inspection of the packets can be achieved by using next-general firewalls (NGFWs). The operation and management (OAM) systems should also be inspected for any malware, which can be achieved by using an anti-malware solution that can also validate user devices to mitigate any risks from user devices impacting the 5GC OAM network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 421, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4880a8db85f3223379f696e849571873', 'text': 'Acronym Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 421, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '89e79d350bf5fcb28a63234dce279092', 'text': 'Acronym Expansion 3GPP 3rd Generation Partnership Program 5GC 5G core AF Application Function API Application programming interface APIGW Application programming interface gateway APM Application performance monitoring AUSF Authentication Server Function BM Bare metal C&C Command and control c2C Command and control CD Continuous Delivery CI Continuous Integration CNF Cloud-native function CPU Central processing unit CSR Certificate signing request DC Data center DDoS Distributed denial of service', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Acronym</th><th>Expansion</th></tr></thead><tbody><tr><td>3GPP</td><td>3rd Generation Partnership Program</td></tr><tr><td>5GC</td><td>5G core</td></tr><tr><td>AF</td><td>Application Function</td></tr><tr><td>API</td><td>Application programming interface</td></tr><tr><td>APIGW</td><td>Application programming interface gateway</td></tr><tr><td>APM</td><td>Application performance monitoring</td></tr><tr><td>AUSF</td><td>Authentication Server Function</td></tr><tr><td>BM</td><td>Bare metal</td></tr><tr><td>C&amp;C</td><td>Command and control</td></tr><tr><td>c2C</td><td>Command and control</td></tr><tr><td>CD</td><td>Continuous Delivery</td></tr><tr><td>CI</td><td>Continuous Integration</td></tr><tr><td>CNF</td><td>Cloud-native function</td></tr><tr><td>CPU</td><td>Central processing unit</td></tr><tr><td>CSR</td><td>Certificate signing request</td></tr><tr><td>DC</td><td>Data center</td></tr><tr><td>DDoS</td><td>Distributed denial of service</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 422, 'parent\_id': '4880a8db85f3223379f696e849571873', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'e4f7386eb7ef4dd89b76833363f2cc5b', 'text': 'DevOps Development and operations DNS Domain Name System DoS Denial of service HPLMN Home public land mobile network HTTP Hypertext Transfer Protocol IAM Identity and Access Management JSON JavaScript Object Notation JWE JSON Web Encryption JWT JavaScript Object Notation Web Tokens LDAP Lightweight Directory Access Protocol LDAP Lightweight Directory Access Protocol MEC Multi-access edge compute MFA Multifactor authentication MitM Man in the middle mTLS Mutual Transport Layer Security NAC Network Access Control NAS Non[nd]Access Stratum NEF Network Exposure Function NF Network Function', 'metadata': {'text\_as\_html': '<table><thead><tr><th>DevOps</th><th>Development and operations</th></tr></thead><tbody><tr><td>DNS</td><td>Domain Name System</td></tr><tr><td>DoS</td><td>Denial of service</td></tr><tr><td>HPLMN</td><td>Home public land mobile network</td></tr><tr><td>HTTP</td><td>Hypertext Transfer Protocol</td></tr><tr><td>IAM</td><td>Identity and Access Management</td></tr><tr><td>JSON</td><td>JavaScript Object Notation</td></tr><tr><td>JWE</td><td>JSON Web Encryption</td></tr><tr><td>JWT</td><td>JavaScript Object Notation Web Tokens</td></tr><tr><td>LDAP</td><td>Lightweight Directory Access Protocol</td></tr><tr><td>LDAP</td><td>Lightweight Directory Access Protocol</td></tr><tr><td>MEC</td><td>Multi-access edge compute</td></tr><tr><td>MFA</td><td>Multifactor authentication</td></tr><tr><td>MitM</td><td>Man in the middle</td></tr><tr><td>mTLS</td><td>Mutual Transport Layer Security</td></tr><tr><td>NAC</td><td>Network Access Control</td></tr><tr><td>NAS</td><td>Non[nd]Access Stratum</td></tr><tr><td>NEF</td><td>Network Exposure Function</td></tr><tr><td>NF</td><td>Network Function</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 423, 'parent\_id': '4880a8db85f3223379f696e849571873', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '763b2444f990e8663a55dd1197d4f0fb', 'text': 'NSA Non-standalone NTP Network Time Protocol OIDC Open ID Connect PCF Policy Control Function RA-VPN Remote access virtual private network RAN Radio access network RBAC Role-based access control REST Representational State Transfer RPC Remote procedure call SA Standalone SBA Service-based architecture SBI Service-based interface SCEF Service Capabilities Exposure Function SCp Service Communication Proxy SDS Secret Discovery Service SEPP Security Edge Protection Proxy SMF Session Management Functions SPIFFE Secure Production Identity Framework for Everyone', 'metadata': {'text\_as\_html': '<table><thead><tr><th>NSA</th><th>Non-standalone</th></tr></thead><tbody><tr><td>NTP</td><td>Network Time Protocol</td></tr><tr><td>OIDC</td><td>Open ID Connect</td></tr><tr><td>PCF</td><td>Policy Control Function</td></tr><tr><td>RA-VPN</td><td>Remote access virtual private network</td></tr><tr><td>RAN</td><td>Radio access network</td></tr><tr><td>RBAC</td><td>Role-based access control</td></tr><tr><td>REST</td><td>Representational State Transfer</td></tr><tr><td>RPC</td><td>Remote procedure call</td></tr><tr><td>SA</td><td>Standalone</td></tr><tr><td>SBA</td><td>Service-based architecture</td></tr><tr><td>SBI</td><td>Service-based interface</td></tr><tr><td>SCEF</td><td>Service Capabilities Exposure Function</td></tr><tr><td>SCp</td><td>Service Communication Proxy</td></tr><tr><td>SDS</td><td>Secret Discovery Service</td></tr><tr><td>SEPP</td><td>Security Edge Protection Proxy</td></tr><tr><td>SMF</td><td>Session Management Functions</td></tr><tr><td>SPIFFE</td><td>Secure Production Identity Framework for Everyone</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 424, 'parent\_id': '4880a8db85f3223379f696e849571873', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '392c32136c64a5f24a4e823478b9aedb', 'text': 'TAM Trust Anchor Modules TLS Transport Layer Security TPM Trusted Platform Modules TTD Time to detect UDM Unified Data Management UE User equipment UEFI Unified Extensible Firmware Interface up Uplink UPF User Plane Function URLLC Ultra-reliable low-latency communication VM Virtual machine VNFM Virtual Network Function Manager VPLMN Visited public land mobile network WAF Web application firewall XSS Cross-site scripting', 'metadata': {'text\_as\_html': '<table><thead><tr><th>TAM</th><th>Trust Anchor Modules</th></tr></thead><tbody><tr><td>TLS</td><td>Transport Layer Security</td></tr><tr><td>TPM</td><td>Trusted Platform Modules</td></tr><tr><td>TTD</td><td>Time to detect</td></tr><tr><td>UDM</td><td>Unified Data Management</td></tr><tr><td>UE</td><td>User equipment</td></tr><tr><td>UEFI</td><td>Unified Extensible Firmware Interface</td></tr><tr><td>up</td><td>Uplink</td></tr><tr><td>UPF</td><td>User Plane Function</td></tr><tr><td>URLLC</td><td>Ultra-reliable low-latency communication</td></tr><tr><td>VM</td><td>Virtual machine</td></tr><tr><td>VNFM</td><td>Virtual Network Function Manager</td></tr><tr><td>VPLMN</td><td>Visited public land mobile network</td></tr><tr><td>WAF</td><td>Web application firewall</td></tr><tr><td>XSS</td><td>Cross-site scripting</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 425, 'parent\_id': '4880a8db85f3223379f696e849571873', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 425, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4697a117611703f5f09174fd626d0500', 'text': '3GPP TS 23.222, “Common API Framework for 3GPP Northbound APIs,” Release 16, v16.10.0, June 2021', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 425, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7c5e651ab6a610d89b295e736aec68d1', 'text': 'APIs,” Release 16, v16.10.0, June 2021', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 425, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a787b09a89534678a5f5aef3ec0996c6', 'text': '3GPP TS 33.501, “Security architecture and procedures for 5G system,” Release 16, v16.7.0, June 2021', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 425, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cc591073372c94d32c531c67f486a6bf', 'text': 'NIST Special Publication 800-190', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 425, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1bacc30a9ea5a9b9c0057bb7e1b6de88', 'text': 'https://docs.docker.com/engine/security/trust/', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 425, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aef9798a7c910b628e1ca885cb3f25aa', 'text': 'https://www.appdynamics.com/', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 425, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6546de97eb72421c59b4e93856b31daf', 'text': 'https://istio.io', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 425, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5ccceb15112b87d91fd6efc4b0663299', 'text': 'Pramod Nair, “Securing 5G and Evolving Architectures,” Cisco', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 425, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8782395769dd408c076d1b6fc96800db', 'text': 'Pramod Nair, “Securing 5G and Evolving Architectures,” Cisco Knowledge Networks, Cisco Public, September 17, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 425, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd27dc5e607c0620dff924a5d6e0399c6', 'text': 'Pramod Nair, “Why 5G Is Changing Our Approach to Security,”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 426, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cc2063ba57f46c193c892b371f77723f', 'text': 'Pramod Nair, “Securing 5G Cloud-Native Deployments,”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 426, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bf912946f3633cf364ca018620e0ff16', 'text': 'Cisco Public, June 10, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 426, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4c4ba41def7215878cb888a81c3c67fa', 'text': 'Open5GCon, September 30, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 426, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1cfca54476058d270100f2ab2482c95e', 'text': 'https://kubernetes.io', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 426, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '95842945a13527e7347b9155193b0f6d', 'text': 'https://www.portshift.io', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 426, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '92f35e88958f431c063d7bd0f3288ca7', 'text': 'https://www.kennasecurity.com', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 426, 'parent\_id': '868f27c0f19f3e95b7f12ddec4d1b1f9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'text': 'Chapter 7. Securing Network Slice, SDN, and Orchestration in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1aa890346e4080da1b5de39b9ce9f16e', 'text': 'After reading this chapter, you should have a better understanding of the following topics:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0313a5f552239f940c24ca541dbd55b0', 'text': '• Threats in SDN, orchestration, and network slice deployments in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0914a154c64224c418c853addffcaff3', 'text': '• Securing SDN, orchestration, and network slice deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '747407b5af0aeef9b4a2ff88b1ef04cc', 'text': '• Real scenario case study examples of SDN, orchestration, and network slice threat surfaces and threat mitigation techniques', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1967b498ba322a93736312dfc04388bb', 'text': 'This chapter will take you through the threat surface and mechanisms to mitigate threats in the 5G network slice and its enablers—software-defined networks (SDNs) and orchestration.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '99105fa1e177e7863cd542774f253fa6', 'text': 'This chapter will be of particular interest to the following teams from enterprise and 5G service providers deploying 5GC and cybersecurity vendors planning product developments and new functionalities to secure the deployment of 5GC:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1f21c0c2286de0b87d4e461d169e23c0', 'text': '• SDN and orchestration teams within enterprises, service providers, and vendors', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '514d160a7d26af20dd9c9a3194bf416e', 'text': '• Automation strategy teams of service providers deploying 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9d121a54588c088e863fa8c3021bf8e2', 'text': '• Security strategy teams within service providers deploying 5G network slice', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f8a8a0d26b6a263f5896f31558d52ee1', 'text': '• Service providers planning to offer network slice as a service (NSaaS)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b7818e6a45abf1aa37acc65ed95b9507', 'text': '• Enterprises planning to monetize the network slice provider marketspace', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'db9a64a2cbad85ff960ec86994e456e4', 'text': '• Security strategy teams within enterprise verticals planning on deploying 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '656d6c1378f05b67083cabf47b722ee9', 'text': '• RAN, transport, packet core, and data center teams involved with 5G strategy', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f1fe4b64f9cd34deed82962890e91c6d', 'text': '• Security architects and design teams looking at secure SDN and automation deployments for 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 427, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3489843d84587b282b30103e79c680c3', 'text': '• Enterprise solution and security architects deploying 5G network slicing on enterprise premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 428, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '630c611986d083a2707f261393d29cf4', 'text': '• Enterprise solution architects and enterprise security architects working with enterprises integrated with service provider 5G networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 428, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1da4a82e3cdd0bf0fb2ea35a8d9cd25a', 'text': '• Government departments looking at regulating security for service providers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 428, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a3f1be69c7bf14dcf260760dd6adbf81', 'text': '• Cybersecurity vendor security architects looking to secure 5GC deployments for their end customers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 428, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fddd9c93223ed000d58d679b19431f7b', 'text': '• Cybersecurity vendor product managers looking for use cases or features to enhance security products to cater for secure 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 428, 'parent\_id': '88c47d8dc4c77afa40573e1cd0464e4e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5f494fbb1d02b331aa8e5b51616d4655', 'text': 'Network Slicing and Its Enablers—SDN and Orchestration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 428, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d44d2428fe08b72af503af91fc6643c', 'text': 'Network slicing is a key concept in 5G. It is the ability to build what looks like discrete end-to-end networks for different 5G use cases or customers. However, one requirement of network slicing is that network functions might need to be shared between slices. For example, the multiple slices might share the control plane, but each individual slice might have its own user plane function. One of the other key requirements of 5G is that the network needs to be designed to be able to offer a different mix of capabilities to meet all diverse requirements, such as high-bandwidth high throughput and low-latency low throughput, at the same time.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 428, 'parent\_id': '5f494fbb1d02b331aa8e5b51616d4655', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd5a5e306fe33d8d5fa0c15f452aac6a4', 'text': 'In legacy networks such as 4G, an Evolved Packet System (EPS) bearer is the level of granularity for bearer-level quality of service (QoS) control. That is, all traffic mapped to the same EPS bearer receives the same bearer-level packet- forwarding treatment, such as scheduling policy, queue management policy, rate-shaping policy, Radio Link Control (RLC) configuration, and so on. One EPS bearer is established when the user equipment (UE) connects to a Packet Data Network (PDN), and that remains established throughout the lifetime of the PDN connection to provide the UE with always-on IP connectivity to that PDN. That bearer is referred to as the default bearer. Any additional EPS bearer that is established for the same PDN connection is referred to as a dedicated bearer. An EPS bearer uniquely identifies traffic flows that receive a common QoS treatment between the UE and a PDN GW for GPRS Tunneling', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 428, 'parent\_id': '5f494fbb1d02b331aa8e5b51616d4655', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e36d76df97895d171668dfdc9e17dc4e', 'text': 'Protocol–based S5/S8. An EPS bearer identity uniquely identifies an EPS bearer for one UE accessing via LTE eNB.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 429, 'parent\_id': '5f494fbb1d02b331aa8e5b51616d4655', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '380ffff06a4e9d4e67dfa6db15696c48', 'text': 'In 5G, the QoS model is based on QoS flows, which are controlled by the Session Management Function (SMF). The SMF performs the binding of Policy and Charging Control (PCC) rules to QoS flows based on the QoS and service requirements. The QoS flow is the finest granularity of QoS differentiation in the PDU session. A QoS flow ID (QFI) is used to identify a QoS flow in the 5G system. User plane traffic with the same QFI within a PDU session receives the same traffic-forwarding treatment (for example, scheduling and admission threshold). The QFI is carried in an encapsulation header on N3, as well as N9 (that is, without any changes to the end-to-end packet header). The 5G QoS model supports both QoS flows that require guaranteed flow bit rate (GBR QoS flows) and QoS flows that do not require guaranteed flow bit rate (non-GBR QoS flows). The 5G QoS model also supports reflective QoS, which enables the UE to map uplink (UL) user plane traffic to QoS flows without Session Management Function–provided QoS rules.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 429, 'parent\_id': '5f494fbb1d02b331aa8e5b51616d4655', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5c1001e110a551a065008d73228626e2', 'text': 'Figure 7-1 illustrates 4G and 5G QoS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 429, 'parent\_id': '5f494fbb1d02b331aa8e5b51616d4655', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '05e0c3e580262bc1d0e1631697798d14', 'text': 'SeCTEn Internet A eNB | == EPS Bearer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 430, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'fafcc88e737c32d527f4e9847542ca08', 'text': '- UE UPF Internet —{ A)) gNB |1 (Il PDU Session', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 430, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2544306414b67e63751b4bbd12dca30', 'text': 'Figure 7-1 4G and 5G QoS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 430, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ce0f766263a4a28677dfb00b1fd18184', 'text': 'As shown in Figure 7-1, the traditional network deployment options did not allow the logical splitting of the network to cater for different use cases. It used the concept of Access Point Names (APN), which is basically the name of a gateway between the mobile network and public internet. Some examples are provided as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 430, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a63833405910b5fd23a3b8da85f1a729', 'text': '2G / 3G APN example: internet.mnc011.mcc123.gprs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 430, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f8b034815c955568c34e0de3550c730', 'text': '4G APN example:internet.apn.epc.mnc011.mcc123.3gppnetwork.org', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 430, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b75a6f4522f494f8758fa5e4c776b2b', 'text': 'The key difference between 4G APN and 2G/3G network APN is the use of “apn.epc” before the mobile network code (mnc) and use of', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 430, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '971114d8f2b1307a670806cee62f266c', 'text': '“3gppnetwork.org” instead of “gprs” after the mobile country code (mcc)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 430, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '395701695d30960ad272bddb3a7bb453', 'text': 'Different APNs are configured in the Evolved Packet Core (EPC), which was then used to identity the QoS or access restrictions on roaming assigned to the user. APN names are chosen by the service providers and some examples of APN names are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 431, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bf834d86e4465b5dec64c37a8f0738a2', 'text': 'APN 1: internet.unlimtedthroughputapn.epc.mnc011.mnc123.3gppnetwork.org APN 2:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 431, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '82f430c01be158778ac626549a3876b8', 'text': 'internet.restrictedthroughputapn.epc.mnc011.mnc123.3gppnetwork.org', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 431, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '49ff6ef8dd8bd945dad5b958a7df0723', 'text': 'In the forementioned example, the configurations for APN 1 in the PGW context allows the users associated with the APN 1 to have unlimited throughput and the configurations for APN 2 in the PGW context restricts the throughput for the users associated with APN 2.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 431, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f91372e0ca714554fe073dd4d36b003b', 'text': 'The PGW will use the APN configuration to select the PDN context and IP addresses are assigned from the IP pool configured in the selected PDN context. The QoS policies are assigned by the Policy Control and Charging Rules Function (PCRF) within the EPC. The key issue in legacy deployments such as 4G was the inability to have a use case–specific dedicated resource. 5G brings significant improvement and flexibility in the QoS, which helps you to deliver ultra-reliable low-latency communication (URLLC) for mission-critical communication services. It also provides you different prioritization levels for different applications, as per preconfigured requirements for specific subscribers or industry/enterprise verticals.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 431, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e079a389f334b43aa1ab907d420bd651', 'text': 'The successful delivery of QoS along with the realization of new use cases, such as URLLC, enhanced mobile broadband (eMBB), and massive machine- type communications (mMTC), requires a tailored logical network using techniques such as network slicing, enabled by multidomain orchestration and SDN architectures to allow the common infrastructure to efficiently support multiple network instances with tailored services. To achieve end-to-end (E2E) automation of the 5G network, an orchestrator should be able to receive the “intent” of the service you require and translate that to real change in the 5G network. The orchestration solution you choose should fully automate the creation, deletion, and runtime modification of network services. It should map design-time service definitions to runtime network operations through a single, flexible data model for a service. The orchestration solution should then derive the minimum network changes required and execute them.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 431, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '56cdc2b6f0857d282b9aad79ac38b481', 'text': 'Orchestration and automation tools have typically been bound to a technology domain: a tool for the packet core network, a tool for the transport network, a', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 431, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b4824b92ce9f8c5860e2b6707ea4fef8', 'text': 'tool for the data center network, a tool for the WAN, a tool for the optical network, and perhaps tools to manage firewalls and other L4–L7 devices. This creates inflexibility and higher complexity for 5G orchestration. The orchestration solution you choose for 5G should span multiple technology domains, allowing you to create and automate cross-domain service chains much more easily and dependably for successful deployment of network slices. Furthermore, orchestration should be done in a loosely coupled manner so that the operations teams responsible each technology domain can work cooperatively with the teams building the service chains.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 432, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3b73ca99d4fc8ffaa7055176f807e814', 'text': 'The actual 5G deployments will require high levels of programmability to ensure that the underlying 5G infrastructure can be abstracted for applications and service. This is enabled by using SDN. Its key concepts (resource virtualization, dynamic initialization, and so on) support the envisioned high degree of flexibility through network slicing. Common abstractions allowed by SDN enable slice resources (networking, processing, and storage types) included in a slice to fulfil a business purpose, while open and programmable interfaces in the SDN and orchestration layers allow dynamic control and automation of network slice creation and operation. This is further realized using new specifications in 5G and new cloud-native deployment methods for 5G Core (5GC). This will help you with flexible configurations and allows multiple networks to be logically deployed on the underlying infrastructure, such as radio, transport, and packet core network, as shown in Figure 7-2.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 432, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c3a9f229a81a2f8d85e173bcfe1ef66e', 'text': "Multi-Domain Orchestration system pmmmmm———— Enterprise / loT MVNMS / SDN GW/ Controller Controller i Slice 1 fmmmmmsmm———— 5GC CNF deployed on Cloud dedicated to Slice 1 Slice 1 i'Ea é Slice 2 w [ \_(( '00 Slice 2 IJ NB (0U+CU) Slice 3 : \_D. 5GC CNF deployed on-premises Tanspo dedicated o Slice 2 ceessssssnana? Slice 3 = 5GC CNF deployed on-premises dedicated to Slice 3 Seasssssssssssssssssasd", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 433, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8d46ea0244d8651adb3ab288b330d42d', 'text': 'Figure 7-2 Network Slice Deployments Enabled by Orchestration and SDN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 433, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0b1ba32a83cdce945cbbd988a9dd59e2', 'text': 'Figure 7-2 illustrates the components required for efficient network slice 5G deployments. The key functions are explained in the list that follows.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 433, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '77df81f90f456ad206fab51c7fc85b69', 'text': '1. Devices: Use cases such as vehicle to everything (V2X), ultra-reliable low- latency communication, and enhanced mobile broadband (eMBB) are', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 433, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0510c82231b120d96d2477ff47c8c3cf', 'text': 'allocated the following slices:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 434, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '000ce21b65e35fbde5f26b58297eb8e5', 'text': '• Slice 1: V2X based on machine-to-machine (M2M) use cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 434, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a4b4b57b070a5900be29f270171bfb0', 'text': '• Slice 2: URLLC use cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 434, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c734cfd314ac927b852b62f466d0eeea', 'text': '• Slice 3: eMBB use cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 434, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '484e069afab4f21aaf83efd22e53331e', 'text': 'The IoT/IIoT devices used in industry verticals such as smart factories enabling M2M and URLLC use cases will be connected to IoT gateways, which provide simple, essential connectivity for assets at mass scale. The gateways will provide connectivity to the 5G network if the devices themselves are not 5G capable. IoT data orchestration software extracts, transforms, and delivers data of connected assets from edge to multicloud destinations with granular data control.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 434, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ec46a80965245d5419a2fc2079559e59', 'text': '2. RAN: You would typically have a multivendor radio access network (MV- RAN) in your 5G network that is managed using Network Management System (NMS), vendor-specific Element Management System (EMS), or configured by an SDN controller. This is indicated in Figure 7-2 as multivendor NMS (MV NMS/SDN controller). A RAN orchestration solution will orchestrate the deployments of virtual RAN components such as Centralized Unit (CU) and Distributed Unit (DU) by integrating with the respective RAN vendor’s NMS/EMS system or third-party SDN solution, as shown in Figure 7-3.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 434, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ea432cfbedcc7145850c9bf49b235768', 'text': '? t API API \\ ¥ f ’ API API \\ 4', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 435, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '99e48c3ed2ce26156da0aa6d667851cf', 'text': 'Figure 7-3 RAN Orchestration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 435, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7961ac9dd759d9f5a39cf68a7d77a843', 'text': '3. Transport and SDN: In 5G, the transport layer is recommended to be programmable and would require a software-defined networking (SDN) approach. Transport devices being deployed in 5G would need to cater for different requirements on the traffic types. In some cases, the transport network would need to handle high-throughput data; in other cases, it would require traffic with demand of low latency with very strict multidomain service level agreements (SLAs) required for a specific traffic profile. This will require dynamic traffic path changes to ensure that the transport network meets the SLAs and converged, end-to-end packet infrastructure, beginning in the access layer and stretching via the network data center all the way to the core, based on segment routing and packet-based QoS. The SDN controller will be integrated using API in the northbound interface with the transport orchestration solution, as shown in Figure 7-4.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 435, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'de913d43308f2cb6694fb6dfa9338016', 'text': "¢ t NBI API API ' (North Bound Interface) \\ { s | «—— S8 API AP| (South Bound Interface) ¥ { Transport Vendor 1 Transport Vendor 2 Network elements Network elements", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 436, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '88e4a585aef6bb6ba2cb3d855a583831', 'text': 'Figure 7-4 Transport Orchestration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 436, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'acdaaed7b295cb47c5e0449ceaf54ae0', 'text': '4. 5G Core (5GC): To meet SLAs and to optimize resources per traffic profile and use cases, the cloud-native-based 5GC control plane (CP) and user plane (UP) network functions (NFs) can be dedicated for specific use cases. In some deployments, you will see 5GC CP NFs being shared to further optimize the number of CP instances required to fulfill the use cases, as shown in Figure 7-5.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 436, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '90865a7576e4f27ac191682647d11a8d', 'text': "(A) (DU+Cy) PCF SMF . NFs dedicated for Slice 1 v 'JOO Slice 1 RAN Common NFs for both slices (-] L SMF . Slice 2 NFs dedicated for Slice 2 Transport Layer", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 437, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ddd5298e86fa453b6dcee213dd85a420', 'text': 'Figure 7-5 Shared Network Slice Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 437, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ab4c7c263ab8cd4da495b1cd3355aa7b', 'text': 'The sample shared slice deployment in Figure 7-5 shows where AMF, NRF, and NSSF are shared for separate slices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 437, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6d0097dd05911947326f00cfc2972fc1', 'text': 'The key features enabling network slice is explained in the list that follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 437, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '486870dd105195cd3c9a1073b2291c65', 'text': '• Network Slice Selection Function (NSSF): Supports the following functionality:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 437, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f5bb2a54f5b6ce62fd78475d6f0d8464', 'text': '• Selecting the set of network slice instances serving the UE', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 437, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd42d57006255ce4c11100d2467220804', 'text': '• Determining the allowed NSSAI and, if needed, the mapping to the subscribed S-NSSAIs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 437, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3559dc8ecff75fe5e8061dc92688c1ff', 'text': '• Determining the configured NSSAI and, if needed, the mapping to the subscribed S-NSSAIs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 438, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c74427f698c32090dc65aa96a748bcd1', 'text': '• Determining the AMF set to be used to serve the UE, or, based on configuration, a list of candidate AMF(s), possibly by querying the NRF', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 438, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e545ca8c2f0b08c69c8c8c2b4a89e995', 'text': '• Network Slice Selection Assistance Information (NSSAI): Used for uniquely identify a network slice. Single NSSAI (S-NSSAI) contains Slice Service Type (SST) and an optional Slice Differentiator (SD) that’s used as an additional differentiator if multiple network slices carry the same SST value.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 438, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5906b491d137415dc8c849cc89ec5fcb', 'text': '• UE Route Selection Policy (URSP): Feature enabled by the Policy Control Function (PCF). Although not a network slice function, it helps inform the network slice status to the UE via the AMF, enabling you to configure a new service to the UE.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 438, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd17dcc59c83146a275fa689ed457ec8f', 'text': '• Multidomain orchestrator: The multidomain orchestrator has the task of interacting with multiple components to orchestrate the necessary changes in the network. The orchestration solution you choose provides a single, network-wide interface to all network devices and services—both physical and virtual—using a common modeling language and data store. It should also let development teams define services and hand them off to operations teams that can then automate service activations and changes quickly and simply, moving from high-level intent to granular device configurations in a single transaction. It should also support the following access options:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 438, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7d357105fa9d10af24de0a4f5aaeb043', 'text': '• CLI: For network engineers who prefer the command-line interface', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 438, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8d3b2830cc61463b8ac85504f37576c2', 'text': '• Web interface: For network engineers who prefer a graphical interface', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 438, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b4508b503d6a6c5a8e4c89df4d44247f', 'text': '• REST: For programmatic access (exactly the same feature set as the CLI and web interface)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 438, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '64bfe9db0c54053d5379e5ab31d1150a', 'text': '• Java/C: For building custom applications and service provisioning logic', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 438, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd739d3a5c662ae0b54668f5aa4496499', 'text': '• JavaScript: For embedding orchestration functions in portals', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 438, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8733db8d7d69e51dd1de873cc191f65d', 'text': '• NETCONF: For importing and exporting XML configurations', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 438, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4c0f8b88cf31371804fbe0cb135f74cb', 'text': '• SNMP: For reading status and receiving orchestration alarms', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 439, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3359ae96214ce0c41cd7d5005d10ea57', 'text': '• Python: At least support Python for scripting network-wide configuration changes', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 439, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c9e99f4fa9e8d0cbadd7e7f84666afc5', 'text': 'Automation, which is very closely tied with orchestration, becomes very important for you because it helps to manage your services and 5GC NFs across their entire lifecycle: from onboarding and deploying new NFs to monitoring health, to scaling up and down instances in response to demand, to automatically remediating issues, to finally spinning down instances and freeing resources for other apps and services. Figure 7-6 illustrates the multidomain orchestration solution interacting with the 5G infrastructure in the southbound interfaces (SBI) covering both SDN-capable and non-capable 5G infrastructure components. 5G CNFs could be deployed on virtual machines (VMs), containers on VMs/bare metal, or on the public cloud, where the 5G CNFs could run as either VMs or containers on top of the compute and storage infrastructure. The northbound interface (NBI) receives the “intent” of the service you require and translates that to real change in the 5G network. It will also be used by third-party application developers to integrate certain software modules within the orchestration layer to enable 5G use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 439, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '01af6fc1195ffc3f1da14d80c38478e5', 'text': 'o 0 ¢ e A 0 A & 0SS Teams Service Teams Design Teams DevOps CI/ CD Scripts & Application [nternal and External teams NBI Multi-Domain Orchestration Layer SBI SBI SDN layer Non-SDN layer P —————— . SDN Layer / W = = = Public cloud M2M/ loT RAN Transport PN CNF & UNF On-premises N CNF & VNF deployments e g b Py S Ly Py VL - ) deployments 5G Infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 440, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '503c884b40478ded8367427ad6c8defc', 'text': 'Service Teams', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 440, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4afa8039b736451a7adf358142984a88', 'text': 'DevOps CI/ CD', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 440, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a2522d104fd31d132de93aefaa399dd', 'text': 'Design Teams', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 440, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'faf1871809c426a6d067e9dadeb17d05', 'text': '0SS Teams', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 440, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b2e20cd029ee9a9523285b851fda2f41', 'text': 'Scripts & Application', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 440, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c36a1c60e4a920506b085beaa5bf1e5c', 'text': 'Figure 7-6 Multidomain Orchestration for Multiple 5GC Deployment Options', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 440, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a075f9ba556950b7e648a87c202c2c6d', 'text': 'Options', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 440, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5bb7e1567bfdce284dbbdcfd7066d14d', 'text': 'The definition of a 5G network slice includes all resources, including radio, mobile core, network data center/virtualization platform, and the transport network. As shown in Figure 7-7, orchestrating a slice successfully requires tight coordination between these different domains, although these domains are very different in their functions, as are the tools needed to control and manage them.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 441, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '596c4b2010f8fde42d9b6835d1557550', 'text': "BT U - .- [ Service Layer .I ............... I ...... Service Creation \\'i - . - e e e e e e . - - | Wmodemwe", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 442, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9856091c2646b2d337ab7a00aab8ed08', 'text': 'Figure 7-7 Depiction of Multiple Domain Coordinating for a Single Use Case', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 442, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2bced15c162bc16190082b005a8abae7', 'text': 'For the orchestration to be successfully deployed, it needs to follow a new approach to succeed by simplifying the control plane, reducing the protocol', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 442, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8612abc0968a2d199145bb201173d281', 'text': 'complexity, and becoming simpler to provision, secure, manage, and monitor. For a pragmatic deployment of a network slice, you need to understand the customer requirement from different industry verticals such as manufacturing, IoT, healthcare, automotive, and so on. Once the requirement is understood, you can then make the template for creating a service for the customer, which will include the type of 3GPP and non-3GPP NFs required and the type of configurations required in the infrastructure components such as the transport and RAN components.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 443, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3c39bc01e9787bff5644448ded80e463', 'text': 'Also, you can enable various commercial models to exploit the advantages provided by the network slice concept. Network slice as a service (NSaaS) is one commercial model you can offer to your customers. This method allows your customers to manage the network slice for themselves by accessing multitenant management of the network slice, where they can configure the required template, as illustrated in Figure 7-8.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 443, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd3fb5f2761ce40e318b7b235497d7ded', 'text': 'P L Ll e L L \\ NSaa$ to Enterprises Management Service Layer ENTN i) Service Creation : : C I - - <—|/ -~ ‘ . | |', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 444, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '14c5c14271617d3f38cf07d8b75f0114', 'text': 'Figure 7-8 Multitenant Management of Network Slice for NSaaS End Customers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 444, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '64d5b6893bcc5edcaa552ba730884bc3', 'text': 'As Figure 7-8 illustrates, enterprises can consume the network slice to fulfill their own communication service needs. Management ENT 1–Management ENT N can be a multitenant management platform provided by the service provider so that the enterprises can manage their own requirement, or the service provider can manage the slice-specific requirements specified by means of an SLA between the service provider and the enterprise. Another model is where your customer uses the network slice as an offering to other customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 444, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8109470aac605a5c20352bcb10996692', 'text': 'These models are typically chosen by the Chief Revenue Officer (CRO) or the external product teams within your organization to monetize the investments in 5G. An example is parts of your network and features such as security, being offered as a service to an industry vertical or an enterprise. The level of NSaaS slice management would depend on the use case and the SLA agreed with your customer. The slice could be fully managed by you as a part of a managed services offering or could be managed by the customer themselves. For example, you offer slice 1 as a service to enterprise A. Enterprise A then resells it to industry vertical A and industry vertical B to fulfill their use cases. In this case, one of the scenarios could be you offering managed services to manage the slice for enterprise A, industry vertical A & B. Another scenario could be you providing access to industry vertical A & B to manage their own slices through a portal provided by enterprise A. Figure 7-9 illustrates an example of slice management when your network slice is used for reselling by your customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 445, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '35b2da02a8e5b863a102887c06ae4484', 'text': 'W R R R R R R R R R R R R R R e e NSaaS to Network Slice Providers Service Layer bl / : : e e o Network Slice Providers INSP) | Enterprises or End customer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 446, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e1cc77324d6f5ca4e41676d72f8f3bec', 'text': 'Figure 7-9 Multitenant Management of Network Slice for NSaaS Network Slice Resellers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 446, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4943e0ee2aa6ab4db12efb70b1241898', 'text': 'Slice Resellers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 446, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e1b941ca8859d9c699e4f8abd4b14c85', 'text': 'As shown in Figure 7-9, the Network Slice Provider (NSP) can use the slice obtained from the service provider to deliver communication services to its end customers. NSPs can configure the slice requirements using the management platform provided, which is multitenant. Management NSP 1 in Figure 7-9 relates to the management layer, which NSP 1 can use to configure slices to provide communication services to enterprises or end customers. The NSaaS offering from the service provider could also include the management of NSP1 being configured and maintained by the service provider using an SLA', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 446, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '642a451dadedb48931e7d4d02973c4c2', 'text': 'between the service provider and NSPs. Note that although NSP is a commonly used term among service providers, it is also called as Communications Service Provider (CSP). Consumers of NSP / CSP are also called Communications Service Consumer (CSC).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 447, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '15a18a17916d8d3c951958912ce8a206', 'text': 'Threat Surfaces in 5G Network Slice, SDN, and Orchestration Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 447, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e4b9ffd9bb55c1d47f1923164b2f108d', 'text': 'This section discusses the key threat surfaces related to the network slice and its dependencies, such as SDN, automation, and orchestration. Figure 7-10 illustrates the threat surfaces in a 5G network with network slice, SDN, orchestration, and automation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 447, 'parent\_id': '15a18a17916d8d3c951958912ce8a206', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a1f2aa91ff38dabb7221a59125be4d62', 'text': '. Management access for " NSaa$ to Network Slice SPN Providers / Enterprise Improper configuration for NSaaS : Service Layer Improper Access Control on NSaa$ | Management \* Improper Access Control APl vulnerabilties — i + APl vulnerabilties - + Side Channel attacks App server vulnerabilties + Transport Sniffing gty + Data Exfitration & hoarding + Side channel attacks + App server winerabilties External SN layer g + Application vulngrabilties U Management layer + DDoS & DoS aftacks \* Improper Access Control APl vul nerabilties . sssssssesssssssenany smanaay 8 ! ¥ Slice 1 | | | Slce 1 ilia \_( asssnss | ) — | (Fmwriow ] | Slice 2 E gNB I (NL+CLN Transport I e e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 448, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36c6c5c8262bf28cf51bed7d9e987806', 'text': 'Figure 7-10 Multidomain Threat Vectors in Network Slice Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 448, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '412a9c8cffdb15659db6ad9cd794cd08', 'text': 'Some of the key threat surfaces illustrated in Figure 7-10 are listed next:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 448, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '493f43c793a21d684d5f1adbcff455d3', 'text': '• Orchestrators are primarily tasked with driving the scale and density of 5G workloads. This leads to risk factors such as workloads of differing sensitivity levels being deployed on same host. An example would be one of the less sensitive workloads, such as an MEC application workload, with direct interface to the Internet being deployed alongside a critical', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 448, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dd2b378068ed4deea9ef777f9f4bb039', 'text': 'workload, such as Unified Data Repository (UDR), which stores subscriber-related data, on the same host.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 449, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ea11a7c748f985e49b8c6be994b043c1', 'text': '• Orchestrators typically use API servers/web servers for API calls. In case of critical vulnerabilities in the web server, the entire orchestration components could be open to attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 449, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3bbc8f7167f3a30ea8f628a987bb4c44', 'text': '• The SDN layer, automation, and orchestration layers being deployed to enable network slicing would require integration with the third-party application and other 5GC network functions using an API. The API, if not deployed following best practices, will bring in threat vectors related to insecure API security risks, such as user- and function-level authorization, excessive data exposure, Broken Object Level, and so on. This becomes more prominent in MEC deployments for 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 449, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '009a1a50757f3a9ea097b73bb429695b', 'text': '• Aside from traditional attacks against servers, DoS and DDoS attacks on the SDN/orchestration/automation layers will impact the service creation leaving your network crippled and will also disrupt the services of the network slice providers and enterprises that are dependent on your network. The vulnerabilities that might cause this to happen would be through traditional attacks on hardware components of the infrastructure, application vulnerabilities, APIs that are not properly secured, and rogue nodes within the architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 449, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b1a86428fb8a27d13fc19f332d206c11', 'text': '• There is an emphasis on flexible software-based architecture enablers, such as software-defined networks (SDNs), to allow optimized slicing and routing for transport traffic; one of the key threats here is the manipulation of the routing table.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 449, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b3f7e554d3f4d879d1cd39808962d8b6', 'text': '• Because all the traffic traverses the network using the SDN network, data exfiltration, data hoarding, and data sniffing are other threats related to the risks in the SDN components.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 449, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7954cf0ad3cc60f03e78f54fb4ed1a29', 'text': '• The SDN controller itself could be a virtual instance built with the cloud- native approach of using an open source software stack that is advantageous to you because it provides flexibility in deployment types, such as VMs and containers, but it also brings in increased risk due to vulnerabilities originating from using unpatched open source software components.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 449, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '14cb149a2ad51968ab57fe30ebfa111a', 'text': '• Unauthorized user access is another risk related to the SDN, orchestration, and automation components within the 5G network. This is applicable to all the layers, such as management, control, and data plane.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 449, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '26118fbe3defd9204833c4ce06a6bddf', 'text': '• NSaaS offers the option of the service management being handled by the enterprises or external third-party Network Slice Providers and opens your network to higher risk if not managed properly.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 450, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ccd4ae1c181f9942cd890c150bf5b983', 'text': '• The network slice could use a shared 5G infrastructure and network functions, or you could have dedicated 5GC NFs for separate slices, but it could share transport and 5G access nodes such as gNB, as shown in Figure 7-11. Improper isolation of network slice components in inter-slice and intra-slice deployments in these types of shared deployments will increase the risk of threats being migrated between the slices or within the slices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 450, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5f31a829f9ec7289c654bf7fa01cf329', 'text': 'Service configuration Service 1 Service 2 Network Slice A Network Slice B Network Slice Network Slice Subnetwork 2 Subnetwork 1 \\ % Core Network B (. Tran;mn Transport Network Y Nodle 1 |/ \\ [ |/ Radio Access Network Node g\\B 1 /A', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 451, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58e7b95a54e83d6d6f40037fbf114f35', 'text': 'Figure 7-11 Network Slice Deployment Example with Shared Transport and Radio Access Node', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 451, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '45c76b8580e1e76f2b9433ae13955e15', 'text': 'As seen in Figure 7-11, two separate network slices are mapped to separate services. At the 5GC level, the same network functions can be allocated to dedicated NFs. The traffic between the access network (gNB) and the 5GC is catered to by a common transport network and, depending on the configuration, might also pass through a shared transport device such as an access and aggregation router as well as a shared access network component such as gNB.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 452, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b00a39ec720c6925accc9b8d090d7bd2', 'text': 'Threats in the SDN Controller Layer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 452, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7786932d461da64b84d73e3d13005faf', 'text': 'The SDN control plane handles all routing protocol control traffic. Protocols such as the Border Gateway Protocol (BGP) and the Open Shortest Path First (OSPF) Protocol send control packets between devices. These packets are destined to router addresses and are called control plane packets.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 452, 'parent\_id': 'b00a39ec720c6925accc9b8d090d7bd2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fbce683b04a210c7ae9d8c2fa0bbe856', 'text': 'Any attacks on the control plane, such as TCP SYN flooding, Internet Control Message Protocol (ICMP) echo requests, and so on, will impact the performance of your SDN controller. Some of the key impacts are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 452, 'parent\_id': 'b00a39ec720c6925accc9b8d090d7bd2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b36bb786393ce28cead2dc47a1d85e78', 'text': '• High CPU utilization or saturation of the route processor', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 452, 'parent\_id': 'b00a39ec720c6925accc9b8d090d7bd2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a5307eca3cced0dcca19f3405b8a718f', 'text': '• Memory and buffer resource exhaustion', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 452, 'parent\_id': 'b00a39ec720c6925accc9b8d090d7bd2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8e75c3556dbf75edace90da68eff48f9', 'text': '• Impact on the services being catered to by the SDN, such as NSaaS, 5G slices catering to your customers (like IoT slices), and so on', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 452, 'parent\_id': 'b00a39ec720c6925accc9b8d090d7bd2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '79f022db1c03815c94dff1d7dd91779e', 'text': '• Crashing the SDN controller or destabilize routing and causing data disruption', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 452, 'parent\_id': 'b00a39ec720c6925accc9b8d090d7bd2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8cea71d46b25b25b225d1be591d6751e', 'text': '• Dropping of legitimate packets due to CPU buffer and memory exhaustion', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 452, 'parent\_id': 'b00a39ec720c6925accc9b8d090d7bd2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '42330a16b642f7a0e66531505a2eda18', 'text': 'Figure 7-12 illustrates the threat surface due to an attacker exfiltrating data using the common SDN network used for different network slices. Depending on your network deployment, there might be multiple protocols being used by the SDN controller to communicate with the network elements and their Element Management System (EMS) or Network Management System (NMS), if any configuration changes are required. Although multiple protocols will be used, such as Locator/Identifier Separation Protocol (LISP), OpenFlow, and Simple Network Management Protocol (SNMP), the majority of the southbound communications from the SDN network toward the network elements would be based on different API architectures such as Representational State Transfer (REST), JavaScript Object Notation – Remote', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 452, 'parent\_id': 'b00a39ec720c6925accc9b8d090d7bd2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1a7b319e6c50aff50dd368543fab8720', 'text': 'Procedure Call (JSON-RPC), Extensible Markup Language – Remote Procedure Call (XML-RPC), and Simple Object Access Protocol (SOAP). Although APIs have been deployed in enterprise and web servers for quite some time, they have not yet been widely deployed in the telecom part of the infrastructure, leading to insecure implementations of the APIs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 453, 'parent\_id': 'b00a39ec720c6925accc9b8d090d7bd2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '2006d3a3c415d8ad9d443985392c8c7e', 'text': 'Service 1 Senvice 2 Service configuration Network Slice A Network Slice B Separate 56 Core Network NFs per slice) L [ o— Attacker Transport SON (Common Transport SON NW for both Network slices) OA; A\\ Access Network | Data (Separate 5G access ONB %)) | Exfilration nodes per slice) cluster 1', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 453, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6d42a9d1c6a8e327c5260cab877b8500', 'text': 'Figure 7-12 Sample Threat in Network Slice Deployment Example with Shared Transport and Radio Access Node', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 454, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0488309f0fc602dca2105ca2f40d5707', 'text': 'The attack surface shown in Figure 7-12 is explained for two sample attacks— one using an API and the other using topology poisoning—in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 454, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5efed3dbbd342398b66e1d1acae3fe9b', 'text': '1. API vulnerability on programmable transport device: As shown in Figure 7-12, the attacker exploits the API interface in the programmable transport device for vulnerabilities such as broken authentication and broken access control. Many of the programmable transport devices support deployment of containers in the device hardware and allow communication using APIs. These third-party containers, which use the built-in general CPU, memory, and storage within the transport device, are susceptible to API vulnerabilities due to weak API implementation with little to no security controls. Some of the weak security mechanisms usually seen in API implementations allow the attacker to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users’ identities due to incorrect implementation of authentication and session management functions. Incorrect implementation of authentication and authorization could also allow attackers access to unauthorized functionality and/or data, such as accessing other users’ accounts, viewing sensitive files, modifying other users’ data, and changing access rights within the container deployed on the programmable transport device.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 454, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0ce7cca0e69e78ae6297c49620f0ca8b', 'text': 'One of the main foundations for the SDN architecture is the centralized SDN controller, which has visibility over the entire topology of the underlying network. One of the key attack surfaces on the SDN controller is the topology poisoning attack, as shown in Figure 7-13.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 454, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd300757a6ad05573f70cad4d8a28a78c', 'text': 'SDN Controller', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 455, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '2997c8f0d3cfd4f8832121b8dee9e7c8', 'text': 'SDN Controller Forwarding plane / Device offline Exfiltrated data O Rogue Device imitating the offline device Attacker', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 455, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4b7f28d1dff14fb62f9b6d1e2c3a6162', 'text': 'Figure 7-13 Depiction of the Topology Poisoning Attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 455, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2084829aa09403c1bc2e186b02e46b0a', 'text': 'Topology poisoning attack vectors rely on the functionality of the SDN controller, which allows network devices such as switches to be unplugged and replaced with a new device or allows changing the location of the device. In this attack vector, the attacker probes the ports to check the state of the device and identify if any devices have been turned offline. Once the legitimate device is detected as being offline, the attacker uses the spoofed network identity of the legitimate device and shows it in a new location. The SDN controller sees this rogue device as a legitimate device and recomputes the flow table to forward the traffic to this rogue device. The rogue device will now act as the man in the middle (MitM). All the traffic flowing through this rogue device can be inspected by the attacker and can be used for malicious activities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 455, 'parent\_id': '4b7f28d1dff14fb62f9b6d1e2c3a6162', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'abfeaef09a9ff189671df311c0d9b683', 'text': '2. Data exfiltration: Both of the aforementioned attack surfaces—exploiting API vulnerabilities and the topology poisoning attack—will lead to data exfiltration or data hoarding, where sensitive information is exfiltrated out of the network. This data could be analyzed by the attacker to understand the identities of the network components and then launch an attack on the network using the most vulnerable components of the infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 456, 'parent\_id': '4b7f28d1dff14fb62f9b6d1e2c3a6162', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1343b17a559c6a1d3e04e6076b160982', 'text': 'DDoS Attacks on the SDN Control Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 456, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f69fbcd1502649b5391ff2e830cca601', 'text': 'Distributed denial of service (DDoS) is one of the most popular attacks on the SDN infrastructure to disrupt the traffic and services of the targeted server or network component. Figure 7-14 illustrates DDoS attacks on the SDN control plane.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 456, 'parent\_id': '1343b17a559c6a1d3e04e6076b160982', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'fd424c662bf231945b95f32e0d118f5b', 'text': 'Orchestrator IAP SON Fabric SON Controller DDoS atfack on SON ﬁg Network Layer Internet R— S— R ~ PR S— ) T MEC Application i’ UPF : B ................... ‘: S—— : :I \\ \\: E\\ P — : i’ | S— ‘: 56C 5G support v 5G Radio 56 Data services services senvices Servioes services', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 457, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c83d2059d525d2c7524776c25396433b', 'text': 'Figure 7-14 DDoS Attacks on the SDN Control Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 457, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dbef34dab35b2b4321009b36ee318a89', 'text': 'Figure 7-14 illustrates an SDN deployment with the data plane providing Internet access to specific network functions and infrastructure components. In this illustration, the network layer allows Direct Internet Access (DIA) for 5G NFs like UPF, including dependent services like DNS. Due to the lack of security awareness with the programmers, the security implementation within the API calls is weak and has increased risk due to weak implementation of authentication and access controls. The attackers exploit this weak API implementation to deploy malicious code that takes complete control of the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 457, 'parent\_id': 'c83d2059d525d2c7524776c25396433b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9d28c906c48fa92711b6f6287a7c5698', 'text': 'switch. Apart from the traffic redirection, which is explained in the entry “API vulnerability on programmable transport device” in a list earlier in this section, the attacker could also launch a DDoS attack on the SDN controller. These DDoS attacks can saturate the CPU within the SDN controller with more requests that it can handle. This in turn cripples the SDN controller, leading to denial of service (DoS) for legitimate requests from other switches and transport devices within the infrastructure being catered to by the SDN controller.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 458, 'parent\_id': 'c83d2059d525d2c7524776c25396433b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'db731355c1df6f25f874054246468859', 'text': 'Threats in the SDN Data Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 458, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4adaf5cd4e86e76e30e4b4a73e4c0d28', 'text': 'The SDN data plane handles all the data traffic. The data plane for the SDN layer in 5G deployments enables data transfer to and from 5G NFs such as User Plane Function (UPF), Centralized Unit (CU), Distributed Unit (DU), and services supporting 5G NFs such as deep packet inspection (DPI) and the data network (DN) for each of the slices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 458, 'parent\_id': 'db731355c1df6f25f874054246468859', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '52d0c0d8d3eb254e41d4e40a865e89ff', 'text': 'Figure 7-15 shows the threat surface due to DDoS attacks on the SDN data plane.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 458, 'parent\_id': 'db731355c1df6f25f874054246468859', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'b8e5a733c700960c3433dbf369d914bf', 'text': 'Orchestrator Pl PR T ......... N SDN Fabric SON Controller DDo$ atiack on SDN Data Plane ﬁg DDo$ attack on SDN Data due to vulnerabiliies in the MEC [ eyspipipupRapy. -Jpupapp— Plang from internet applications deployed in 5GC Network Layer .............. B N Oy MEC Application (o] o oT DI T ................... E e JT— C—— i L——— : g LTR—— : T : 5GC 5G support SG N6/ SGi 5G Radio services services Services Services services', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 459, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b2d6d3b3b4be234f73be51a521176a94', 'text': 'Figure 7-15 DDoS Attacks on the SDN Data Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 459, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '08ad29b04156bfbc0deca56aa9e8bc12', 'text': 'Figure 7-15 illustrates two separate attacks on the data plane of the SDN controller, which caters for the data forwarding for the underlying 5G NFs and infrastructure components. Descriptions of the two separate attacks follow:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 459, 'parent\_id': 'b2d6d3b3b4be234f73be51a521176a94', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '328e154b9ea22f500e417831abfb2441', 'text': '• DDoS attacks originating from internal network: The SDN data plane within the transport SDN network allows Direct Internet Access (DIA) for User Plane Functions (UPFs) for fulfilling ultra-reliable low-latency', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 459, 'parent\_id': 'b2d6d3b3b4be234f73be51a521176a94', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e43e457e4eded93b3223637494858c7a', 'text': 'communication (URLLC) use cases. Figure 7-16 illustrates the attack on the SDN data plane by devices in the internal network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 460, 'parent\_id': 'b2d6d3b3b4be234f73be51a521176a94', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f7086f28c9ae920bf7d909a0040d7e79', 'text': 'Y L AN\\ ppln', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 460, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd9913ad68dbf34da7b2b458ca0e84544', 'text': 'Ay L \\] MEC & 5 ¥ Appln', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 460, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '705cec8f4521d60f1081c1a9128b4f37', 'text': 'EEe E2e \\ \\MAAW/A MEC d iy Appin', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 460, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'aa6a7445bf32772b35526972cb399029', 'text': 'Figure 7-16 DDoS Attacks Due to Malicious Code Injection in MEC Applications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 460, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '900e711b2299f565bbb7897b73aa4dbf', 'text': 'Applications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 460, 'parent\_id': 'aa6a7445bf32772b35526972cb399029', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '907d528580fa99b732fd4b1e7c4cda53', 'text': 'The steps in the attack illustrated in Figure 7-16 are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 460, 'parent\_id': 'aa6a7445bf32772b35526972cb399029', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '057a93829c2e2e2fbdf76054bf9359fb', 'text': 'a. The attacker exploits the vulnerabilities in the deployed 5GC NFs (non- 3GPP or 3GPP). The attacker can exploit the vulnerabilities in the API implementation or can exploit the vulnerabilities in the open source software stack being used to build 5G NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 460, 'parent\_id': 'aa6a7445bf32772b35526972cb399029', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0f752a3e327d07f256666a06a179b5f2', 'text': 'b. The malware deployed by attackers are of multiple variants. Some malware methods could be fileless. In fileless malware-based attacks, the malware is loaded into memory and then executed. This method could also open a backdoor to the attackers or command and control (C2C) servers, which can now control all the NFs/MEC applications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 460, 'parent\_id': 'aa6a7445bf32772b35526972cb399029', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8a12b1e4ddd736c42bd37012c34dea0e', 'text': 'c. The C2C servers can now launch a DDoS attack toward the SDN data plane that can saturate the CPU or exhaust the device’s resources such as memory and storage. As the DDoS attack is initiated from the NFs deployed within the infrastructure, it can be considered a DDoS attack originating from your internal network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 460, 'parent\_id': 'aa6a7445bf32772b35526972cb399029', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b2aae18a0216f018ac3e53e9e6d5cf56', 'text': '• DDoS attacks originating from external network: The SDN data plane within the transport SDN network enables the connectivity of various 5G NFs with different data networks (DNs) based on the slices, such as IoT and so on. One of the key risks from the networks serving the IoT devices are the DDoS attacks from botnets that take control of the IoT devices due to unpatchable vulnerable firmware, nonexistent or inadequate passwords, or unsecure interfaces on configuration management (CM), performance management (PM), or fault management (FM) communications. These DDoS attacks could be directed at the SDN data plane that provides connectivity between the DN and the NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 461, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '857d17cd8388d44782f4d07b1d848797', 'text': 'Threats in Orchestration Layer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 461, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3dbd9ef28bf9d1226db6a67ead2ecce3', 'text': 'Figure 7-18 illustrates the criticality of risks related to the orchestration layer. You will see these risks explained in many different use cases throughout the chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 461, 'parent\_id': '857d17cd8388d44782f4d07b1d848797', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '686fba7fe0c43f199134c58f8b91f783', 'text': 'Service Layer o Aftacker MitM attack API + Exploiing AP! vulnerabilties + Privilege escalation atiacks + Unauthorized access to slice [esources Orchestration Layer + Delete all resources slice 1 + Update the Slice resources with malicious patch updates + Delete licenses of NFs in slice 2 \\ SN Layer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 461, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ef5d6f5041ae0f74291c404dafd94f4c', 'text': 'Figure 7-17 Threat Surfaces in Orchestration Layer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 462, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bbdb8cadefc60f83aff57494e18a3b45', 'text': 'Figure 7-17 illustrates some of the key risk vectors related to the orchestration layer in 5G network slicing deployments, as explained in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 462, 'parent\_id': 'ef5d6f5041ae0f74291c404dafd94f4c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ad3764ba5749bf7b83d5c02c36d43a78', 'text': '1. The attacker could perform a man in the middle (MitM) attack in the API calls in the northbound interfaces (NBIs) implemented from the orchestration layer toward the service layer, where the attacker deliberately indicates that the application in the service layer only supports a weaker encryption protocol. The communication packets sent using the API are then encrypted by a weaker protocol, and the attacker can now easily decrypt the encrypted packets and exfiltrate the information for further analysis and then carry out attacks against the critical infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 462, 'parent\_id': 'ef5d6f5041ae0f74291c404dafd94f4c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '173cc1300a792b9618dd1a87b860c816', 'text': '2. Another risk shown in Figure 7-17 is the attacker gaining unauthorized access to the orchestration layer due to weak API security or by exploiting the weak security controls implemented in the API server within the orchestration layer. Some of the key risks related to this attack surface are unauthorized access gained by exploiting the vulnerabilities in the web server being used for API calls and the weak implementation of the API itself, as explained in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 462, 'parent\_id': 'ef5d6f5041ae0f74291c404dafd94f4c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a766f479c64d269637e7cee57fd4885', 'text': '• Once the attacker gains unauthorized access to the orchestration layer, a privilege escalation attack could be performed whereby the attacker has admin rights and can perform actions like deleting the network functions related to a critical slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 462, 'parent\_id': 'ef5d6f5041ae0f74291c404dafd94f4c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3bb9b307dd67ab33abc97e2fc33292ae', 'text': '• Another risk vector could be the attacker choosing to force a patch update of the network functions in a specific slice. The patch update can be forced with a malicious patch that inserts malicious code into the network function, and the attacker could then start exfiltrating sensitive information from the network to an external server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 462, 'parent\_id': 'ef5d6f5041ae0f74291c404dafd94f4c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e1a6e9761a5c6272778a5df6c5218f19', 'text': '• The attacker could also perform actions such as deploying license exhaustion codes in the infrastructure, wherein the entire license file is erased in perpetuity, which means that each time any software is deployed on a specific host, the malicious code deletes the license files. These kinds of attacks are hard to detect, and the user of the host might find it difficult to understand that malicious code is performing such actions from the orchestration layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 462, 'parent\_id': 'ef5d6f5041ae0f74291c404dafd94f4c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f7800603097ac513f0d93d0e99d857d6', 'text': 'Insufficient Slice-Level Isolation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 463, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '21989a287e9828b2fa27c0edbfe1f8f2', 'text': 'When you deploy slices to cater for the 5G use cases, there might be many devices with different capabilities within the individual slices. Some of the devices within the slice served by 3GPP access networks will perform primary authentication between the 5G device and the 5GC for PLMN access, authorization, and authentication. Other devices that are served by non-3GPP access networks will be able to access your 5GC, in which case a new 5G function called the non-3GPP interworking function with IPsec capabilities needs to be deployed. This unified authentication framework in 5G enables access network–agnostic authentication for the devices being served by your 5G network but does not entail slice-level authentication.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 463, 'parent\_id': 'f7800603097ac513f0d93d0e99d857d6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ca0894168f50d28affc33c0cb1ca835b', 'text': 'Figure 7-18 shows the threat surface due to insufficient isolation at the network slice level.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 463, 'parent\_id': 'f7800603097ac513f0d93d0e99d857d6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '065fdb07a796bb49b0c1de939052b22d', 'text': "((A)) B (Du+Cul NFs dedicated for Slice 1 0 v Improper / non Existent Slice 'JOO Slice 1 level N & authentication - W = Slice 2 Transport Layer NFs dedicated for Slice 2 UE 1 initially consuming fesources from entitled UE 1 within UE 1 authenticated Slice 2 using 3GPP slice (Slice 2) credentials", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 464, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e4aaddf6a2e5789c06848e9c4ac533c4', 'text': 'Figure 7-18 Threat Surfaces Due to Insufficient Isolation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 464, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a02a5faed3956a5ea07a570edde5e438', 'text': 'To provide better clarity on the attack vector in actual deployment, Figure 7-19 illustrates the physical diagram of the functional diagram illustrated in Figure 7-18.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 464, 'parent\_id': 'e4aaddf6a2e5789c06848e9c4ac533c4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '26251afc2133e69aca92af853ce71949', 'text': '((A)) dd NB - Internet (u+Cu) ToR ToR switches switches MEC Backhaul Centralized 5GC @ UPFUPF UPF AMF AMF AV SMF SMF SMF 3pa kil pany 3 pany Appln Appin Appln Slice Slice Slice Slice Slice Slice Slice Slioe Slice Slice 1 consumes Slice 1 Slice2 Slce 3 more resources from ohh GHEG il the host CPU il impacting —\_— ﬂﬂﬂ performance for o\\ 0 (RN Slice 2 NFs uuuu', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 465, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '66936cf450b5cb1f757964ce8c7279b5', 'text': 'Figure 7-19 Impact of Insufficient Isolation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 465, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d62698aec8e4574e8b00f320ea0ae83', 'text': 'As shown in Figure 7-19, in real scenarios, similar functions are grouped together in same NFVi. Due to inadequate isolation between slices, unauthorized devices or user equipment (UE) will be able to access other slices that those UEs are not entitled to access. This will lead to consumption of resources of the network slice planned to cater for another use case, thereby causing denial of service (DoS) to the devices that had been originally entitled to access the impacted network slice. Figure 7-19 is further explained in following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 465, 'parent\_id': '66936cf450b5cb1f757964ce8c7279b5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8db648e01b7de7d43e2e8d29786755e0', 'text': '1. User Equipment 1 (UE 1) is a device within network slice 2, which is authenticated using the 5G unified authentication framework defined by 3GPP, as shown in Figure 7-20.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 465, 'parent\_id': '66936cf450b5cb1f757964ce8c7279b5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ca34eadff7d2928fcb06dca07527da05', 'text': '((A» g\\NB (DU +CU) 3GPP Access Network SIDF/ AMF / SEAF A USF [ uom ARPF N3IWF UE1 ﬁ iF Non-3GPP Access Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 466, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ef2082740ad75cff8228607278b23209', 'text': 'Figure 7-20 3GPP and Non-3GPP Network Authentication for UEs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 466, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '00627c267dff71c907bfb19c7da4a316', 'text': 'The network components shown in Figure 7-20 and the network authentication options are explained in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 466, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd24ff83001989e50d1acff50c035ce70', 'text': '• UE: User Equipment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 466, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '00067fbf5bbc9d8de124b44a7de29a7a', 'text': '• 3GPP Access Network: Access network with cellular technologies specified by 3GPP (for example, 4G and 5G)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 466, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9de74626a13ebc7a16c2ff0345dd2264', 'text': '• Non-3GPP Access Network: Access network with wireless technologies not specified by 3GPP (for example, Wi-Fi)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 466, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9c863b991c22dbd61ebec89fc4292a74', 'text': '• AMF: Access and Mobility Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 466, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eebf2f1cfa51c6cbe4989ab8feafe3d0', 'text': '• SEAF: Security Anchor Function', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 466, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9eb5b75c396b7c20f5be6c34a0325694', 'text': '• N3IWF: Non-3GPP Interworking Function, which is responsible for interworking between untrusted non-3GPP networks and the 5G Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 467, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5853168aa62669fd71e17d1dfe502ced', 'text': '• AUSF: Authentication Server Function, which performs authentication of UE in the home network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 467, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2faf9d8e41b35f3a7f474b2fe76bd372', 'text': '• SIDF: Subscriber Identity De-concealing Function, which is responsible for decrypting Subscriber Concealed Identity (SUCI) to reveal the Subscriber Permanent Identifier (SUPI).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 467, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e63137037a214d186340f91ce52f0a3f', 'text': '• UDM: Unified Data Management, which performs user verification handling', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 467, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '63ca6c0f4bcdc2f08406977f4e84ec05', 'text': '• ARPF: Authentication Credential Repository and Processing Function, which is responsible for generating 5G home environment authentication vectors (5GHE AV) based on the subscriber’s shared secret key.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 467, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '011e5a68125919efe7f649d9de4b280b', 'text': '2. As shown in Figure 7-20, when UE 1 served by the 3GPP access network, the UE is authenticated using a protocol such as Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) by encapsulating it in Non- Access Stratum (NAS) messages between UE and AUSF for verifying the pre-shared key (PSK) or verifying each other’s certificate, with SEAF functioning as a transparent EAP authenticator. When UE 1 is being served by non-3GPP access network, then N3IWF will provide secure interworking between the UE and the 5GC. UE 1 performs registration using the IKEv2 SA establishment procedures; once registered, UE 1 will then carry on with the NAS signaling with 5GC network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 467, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '81cd9cfbe0421078e8df670686159465', 'text': '3. The device UE 1 would consume the User Plane Function (UPF) resources from the allocated slice, which is preconfigured with the required QoS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 467, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b01d2457cb5c2d6eae2797f66e28ff23', 'text': '4. The network deployed does not use any slice-specific isolation mechanisms that allow devices from either slice to consume the services of other slices, as shown in Figure 7-19. The services could be edge applications and any function such as UPF. Due to improper slice-level isolation and the nonexistence of slice-level authentication, UE 1, which was originally dimensioned for slice 2, now consumes the resources allocated to slice 1. This unauthorized access of slice 1 by UE 1 will cause a DoS for legitimate user equipment trying to access slice 1 due to resource exhaustion.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 467, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cae024d9d8835fe27a7cd45dad7fc3e9', 'text': 'In deployments where slice-level authentication and isolation are not provided between critical infrastructure slices and consumer IoT slices, the impact on the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 467, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8f0017b00f3dbd0c2973cd78b1e99020', 'text': 'network could be severe, leading to revenue-impacting outages and service impacts.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 468, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e02e751a3f5d542c252a1c8aaa8ae51e', 'text': 'Threats in NSaaS Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 468, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0e7e430089e0241b61f3a45ea942a69e', 'text': '5G network slicing allows allocating dedicated or shared network resources to fulfil requirements of a particular application or use case. You might also offer customized services to the service consumers based on the network slice as a service (NSaaS) model, as described in 3GPP TS 28.530. The customized services offered are characterized by the network slice’s properties, such as radio access technology (RAT), bandwidth, latency, reliability, guaranteed/non- guaranteed QoS, and so on. However, security-related properties are not addressed by TS 28.530.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 468, 'parent\_id': 'e02e751a3f5d542c252a1c8aaa8ae51e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '46c66011b9b000ca64a48e320b2e307d', 'text': 'You could use the NSaaS model to monetize your network slices by providing the aforementioned customized services to either network slice providers (NSPs) or to end enterprises directly. Service providers could also provide managed services such as configuration and maintenance of slices for NSPs or enterprise customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 468, 'parent\_id': 'e02e751a3f5d542c252a1c8aaa8ae51e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7107e61485df51aa00bf163111d8dbbe', 'text': 'Figure 7-21 shows the threat surface due to improper security controls for NSaaS services.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 468, 'parent\_id': 'e02e751a3f5d542c252a1c8aaa8ae51e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '049a9139edeab5636d74642b9868e419', 'text': 'sesssssssssssasanans memmmmame———— Jodsues H (na+na) 55" ) g9 w 3015 88UBJa 109 7.8n0y Jodsuel| L.\_l @@ m m | %om \_\_o%cs I Aﬂ a0y g@\_s Semessenennnnns Nesmsmsscsssesnan- ] Jofey NS 1o/ ONEASaYRI() UBLOGHI - - l \\ \_o>m4 m 2019 asudiapu3 YomaN astidieju3 g [ Temetiue | Y., - / 901G 35Uajaq 1109 J0 Lonaian nazlouineun', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 469, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bda85f67f620959c4755add2d7ca7e01', 'text': 'Figure 7-21 Unauthorized Slice Access in NSaaS Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 469, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '95557da6df171301a8cfc418940e2b51', 'text': 'While providing the option for the NSPs and enterprises to manage their own slices, service providers will usually provide a multitenant management platform that can be accessed by the users (NSPs and consumers of NSPs). The configuration changes can include modification of QoS configurations, RAT selection, and other customizations for the slices. Due to improper access controls being implemented by the management platform, it introduces increased risk of users from one of the enterprise slices performing an unauthorized modification in another slice. As depicted in Figure 7-21, the user or an attacker from an enterprise slice first performs a basic access control and accesses the enterprise slice. The attacker then goes ahead to access the management service layer of a critical infrastructure slice such as the defense network slice and makes changes to the slice, such as deleting the slice or changing the QoS, which might lead to service degradation or cause a DoS for the users and devices of the critical infrastructure slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 470, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d947b539abd1457758d8ba25e574f1d', 'text': 'APIs are used for the exchange of information between external entities such as enterprises, network slice providers, third-party application developers, and the service providers. APIs are very efficient mechanisms if implemented in the right way following the development and deployment best practices; however, a majority of the API implementations are done improperly and increase the risk to your infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 470, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cfd5b4d0aa81027361b4c24646919e82', 'text': 'Figure 7-22 shows the threat surface due to improper API implementation with external applications and web servers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 470, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd415f77503a594af0ac0a4fa160ea08d', 'text': 'API Server T LD LD LN 4 API il Layer M M E - - - - - - - API External Malicious Mutti-Domain Orchestration layer Application / Application Server “a API Attacker ............................................... A amemenene NEF P Slice 2 Transpon Route 1 0F (A) E E Slice 1 i l \\ Transport ] gNB - Neeseusssascsssar (DU+CU) e SRS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 471, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0e8ed77bee14ebef6ab75a6970ffb532', 'text': 'Figure 7-22 Exploiting API Vulnerabilities in NSaaS Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 471, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4fddaf33d2094e778edbfc7315bc86db', 'text': 'As shown in Figure 7-22, API calls will be used by external users, devices, and servers to communicate with the different entities of your network exposed to the Internet. Here are some examples:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 471, 'parent\_id': '0e8ed77bee14ebef6ab75a6970ffb532', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3b5127e58de8b22088c2526cfbb6623b', 'text': '1. Service layer management functions can be accessed by an authorized external entity to perform configuration changes as required by the slice', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 471, 'parent\_id': '0e8ed77bee14ebef6ab75a6970ffb532', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fc39bd0ef984e7e6805de7d98d83fe3c', 'text': 'provider or slice owner. The key threat vectors in the service layer are data leakage and access to the management of the unauthorized slice due to insufficient authentication and authorization within the API implementation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 472, 'parent\_id': '0e8ed77bee14ebef6ab75a6970ffb532', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a48cfea4b370fe3d03bcbab16668ece5', 'text': '2. If the service layer is provided by an external management vendor, then northbound API integration of the external management vendor and the orchestration layer needs to be implemented, as shown in Figure 7-23.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 472, 'parent\_id': '0e8ed77bee14ebef6ab75a6970ffb532', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd0d2c4dc52ae64f67c9fef691e1684d7', 'text': 'W e e e e Senvice Layer provided and managed by external vendor l l - N N NN NN N N NN NN A N RN SN S S e A A A Attacker Service Provider - - e e o e e e ¢ Network API Server Mult-Domain Orchestration layer i SDN Layer { S ——— AENEE \\ D = o] & T W o =] = N2M /ToT PNFs = Public cloud RAN Transport On-premises CNF & UNF Annlaumanta CNF & VNF deployments ——— —— —— —— — — — — —— — — —', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 473, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '74464fe657bef4093015a6e9594600a9', 'text': 'Annlaumanta', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 473, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '25b6758babc90ceb4deed4a5c58cacb7', 'text': 'Figure 7-23 Exploiting API Vulnerabilities in Multidomain Orchestrator', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 473, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9f36582049bb975a7619d34176852ceb', 'text': 'Improper implementation of the API in this layer could lead to unauthorized modifications in the orchestration components. An attacker could exploit the broken authentication vulnerability within the API implementation to perform unauthorized actions such as deleting NFs, thus causing service interruptions, DoS, or network-level outages.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 474, 'parent\_id': '25b6758babc90ceb4deed4a5c58cacb7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '77246dad52326da7e24a0df4ebfb1e4a', 'text': '3. The SDN and automation layer can be integrated with cloud-based services such as security functions using an API interface. Northbound APIs can be used to integrate the SDN controllers to cloud-based automation stacks external to the network, such as Puppet, Ansible, Chef, and so on. Improper security controls during API implementation at the SDN layer could lead to successful DDoS attacks. Figure 7-24 shows the threat surface due to improper implementation of internal API calls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 474, 'parent\_id': '25b6758babc90ceb4deed4a5c58cacb7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '6dcccbcfba43bcb36e15a63ec30630f7', 'text': 'SDN Controller INWAR MitM attacks 0 il ) —A Attacker om O fa == == 5GC VM 5GC Container sl deployment deployment —— — — — 5GC NFs cloud deployment 5GC NFs On-premises deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 475, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '188add666d4dcfcd6cf3da7555f6b5d1', 'text': 'Figure 7-24 Exploiting API Vulnerabilities in SDN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 475, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '17d16e018bbfb9508b04917eff608f3a', 'text': 'As shown in Figure 7-24, the SDN layer you deploy for 5G should cater for the on-premises network functions and dependent infrastructure components and the 5G 3GPP and non-3GPP components deployed on the cloud. Users should be able to access the SDN controller using the user interface (UI) or by utilizing API calls. Many APIs lack encrypted', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 475, 'parent\_id': '188add666d4dcfcd6cf3da7555f6b5d1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2ea720da1aeab2e6540c3729cf0f47d1', 'text': 'communications between the API client and API server in SDN deployments. Attackers exploit such vulnerabilities through man-in-the- middle (MitM) attacks. Attackers can also intercept unencrypted or poorly protected API transactions between the API client and API server in 5G SDN deployment to steal sensitive information between the 5GC NFs and SDN or to alter data being transferred between the 5GC NFs and the respective SDN layers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 476, 'parent\_id': '188add666d4dcfcd6cf3da7555f6b5d1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '132680b16b016fbc1fef0cdc8d269144', 'text': '4. Network Exposure Function (NEF) is used to expose the 5GC NFs to external Application Functions (AFs) using an API. This implementation helps the third-party application ecosystem to evolve and innovate various applications that can be built for 5G use cases. Improper implementation of the API could lead to attackers exploiting the API vulnerabilities, such as passing on more information in the error codes as well as improper access and authentication controls in APIs. These could provide more information about the underlying 5GC NFs and could lead to data exfiltration and data hoarding by the attackers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 476, 'parent\_id': '188add666d4dcfcd6cf3da7555f6b5d1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'aaf955b2394d31c37298b30e5a344f42', 'text': 'Mitigation of Threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 476, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'af216242d7e5d7410d1262a0b8348630', 'text': 'Figure 7-25 illustrates the key components and features of the end-to-end (E2E) secured architecture based on true zero-trust principles.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 476, 'parent\_id': 'aaf955b2394d31c37298b30e5a344f42', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '6e353589b04efff314b78cd7a25b4623', 'text': "J End to End Secured using Zero Trust Principles precccccssssssccssnane E2E Vishlly / + Multi-Factor Authentication + DN Monitoring / + Application Enforcement + Access & Policy + Encrypted Traffic Analysis \* Vulnerabilty Management | + Slice solation & + Data Exfilration detection + Forensics 4 + Anomaly Analysis 4 Service Layer t Mu fi-Domain Orchestration Layer t SDN Layer Container NGFW ~ i '\_Orchestration \\ VIM \\?';.. i % g{ ............. a :é ﬁ :‘ :E ,E 5G Infrastructure", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 477, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'edc53dd2674529b235ecaad4dd16eada', 'text': 'Figure 7-25 Key Security Controls for E2E Secure Network Slice Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 477, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed5f444a35e143c8ed46f4369f3fe359', 'text': 'The key components of the end-to-end secured architecture for SDN, orchestration, and automation are explained further in the sections that follow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6c1e527ab4d1140a9a9cce64c1d0104a', 'text': 'Trusted Components', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8974823252ba849a8708759f359ecd8f', 'text': 'SDN, orchestration, and automation should be secured via a defense-in-depth approach and should have undergone several security verification cycles by following the secure development lifecycle (SDL) process. This is the strong foundation of any zero-trust principle. The SDL process will ensure an increase in product resiliency and trustworthiness. The combination of tools and processes introduced during the development lifecycle promotes defense-in- depth, provides a holistic approach to product resiliency, and establishes a culture of security awareness. This secure product development and deployment practice should include inherent design and development practices, testing the implementation, and creating a set of recommendations for deploying with maximum security. The software development process should be ISO 27001 certified.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'parent\_id': '6c1e527ab4d1140a9a9cce64c1d0104a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7f24ab979388b6d54d0660c4bf8af441', 'text': 'Your chosen SDN, orchestration, and automation vendors should harden the software and hardware with attention to the following:.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'parent\_id': '6c1e527ab4d1140a9a9cce64c1d0104a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c620f2338e70698095622d4e24046e20', 'text': '• Minimum attack surface (no unnecessary open ports)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'parent\_id': '6c1e527ab4d1140a9a9cce64c1d0104a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cc7b680d5f27e8b366db390b2bcd0667', 'text': '• On-demand password reset', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'parent\_id': '6c1e527ab4d1140a9a9cce64c1d0104a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bf7e2550b34bf1b4b3d4e2ed8762fbab', 'text': '• Randomly generated passwords', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'parent\_id': '6c1e527ab4d1140a9a9cce64c1d0104a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fbdbf3bf2d2cf55ca618e1312044f103', 'text': '• Transparent updates of security patches', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'parent\_id': '6c1e527ab4d1140a9a9cce64c1d0104a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e8984a0f4c424a3ba6c273e4ed70d9c4', 'text': '• SELinux (host level) always enabled', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'parent\_id': '6c1e527ab4d1140a9a9cce64c1d0104a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '96bce86035045d3afdfbcd50a765d2be', 'text': '• SSL support', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'parent\_id': '6c1e527ab4d1140a9a9cce64c1d0104a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e8782c67dec401a9d117dd433474b1cf', 'text': '• TLS support', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'parent\_id': '6c1e527ab4d1140a9a9cce64c1d0104a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f8723e81b739ab219055952444b19e0c', 'text': '• Host-based firewalls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'parent\_id': '6c1e527ab4d1140a9a9cce64c1d0104a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '74cd91d28d4c13aadc28564939a26699', 'text': '• Immutable containers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'parent\_id': '6c1e527ab4d1140a9a9cce64c1d0104a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '021e0975cb13559bd9d05f95e8b22a3d', 'text': '• Non-root containers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'parent\_id': '6c1e527ab4d1140a9a9cce64c1d0104a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'text': 'Securing Orchestration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 478, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4afa4874f451466cb1dc627d01084c1a', 'text': '5G will massively increase the size of networks, requiring support of multiple domains, and bring levels of change not seen in previous generations of fixed or mobile networking. To secure the orchestration layer, you will require a layer of security control on top of the security capabilities offered by the orchestration solution itself.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 479, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '10cb9389f0b427989d7b1141e984c8d3', 'text': 'Your chosen multidomain orchestration vendor should provide you with the following security capabilities:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 479, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3a335ca70605d7b9c7b74cadb610a8f5', 'text': '• Comprehensive lifecycle service automation to enable you to design and deliver high-quality services faster and more easily across different domains, such as transport, network data center, and mobile core, all of which could be components of a 5G network slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 479, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1ff9b10e2ed7a21592bbb15ba5bb066b', 'text': '• The ability to provision assurance systems, deploy virtual probes, and so on to ensure that service monitoring is in place.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 479, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '55e342c87005033f7a724f72848e0c6f', 'text': '• The ability to embrace and collect massive amounts of data from different data sources and protocols, including leveraging of streaming telemetry for real-time visibility of the network infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 479, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '281885d21e6cc5301c6b6abedd0af7c6', 'text': '• The ability to discover the network status for each service and render it logically as well as geographically for the operations team.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 479, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '80f41f68009646ed2884886bb407f00a', 'text': '• Logs such as developer logs, audit trail logs, web interface logs, device communication logs, and XPath logs for any forensics or auditing purposes.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 479, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eb7a5c1834ed4019c606cfb68134a2d4', 'text': '• If segment routing is used, the orchestration solution should provide views for segment routing overlay, segment routing policies, and the underlay network, as well as deliver aids and reports to you, which are key for avoiding issues or for expedited remediation when needed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 479, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd52ed2a2a42eea433c851e7b1af1b2da', 'text': '• For secure CI/CD, the orchestration solution you choose should provide following functionalities:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 479, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dc42a938e492c808bfc6484ce47ed774', 'text': '• All of your source code must be stored in version control.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 479, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '76bd7cdfbc88ad8a4c4e1145283ffdc3', 'text': '• Automatic builds must be triggered on each commit.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 479, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '94365dee87538cdc9a04659f05d4357e', 'text': '• Builds must be stored in a special artifactory.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 479, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e7261674ecfe09ee546edb6ed0adbd1d', 'text': '• An automated deployment from build to production should be provided.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 479, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed2f283a028d2177287d3bf7d82d18a5', 'text': 'Apart from the preceding security capabilities supported by the orchestration solution, you will require the key security controls illustrated in Figure 7-26 and explained in the list that follows to protect your orchestration layer:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 480, 'parent\_id': 'f8ae9564f8af2e76aca0fe654917bbbd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '95eb20f5bc5c894860ada1aab7f508f8', 'text': '0 0 0 Security Controls to o A A secure orchestration s O 0SS Teams ~ Service Teams Design Teams DevOps CI/CD Scripts & layer Application ] Global Policy & IAM RBAC - API GW | WAF Multi-Domain Orchestration Layer License and Patch Non-SON Management layer / TLS\\ Validation ananasasas NI L L L s s s e s s s as n s a sy Compliance, and Auditin SDN Layer . j E2E Visibity and 4 O | anomly detection ((A)) ﬁ M2M /loT RAN Transport Fs Public cloud', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 480, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '65e1254a2d0ac3723d1465fc0f6aaf5f', 'text': 'Figure 7-26 Key Security Controls for Secure Orchestration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 480, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b50fe2d31e0e02218a47090e9c8a7d74', 'text': '1. Granular access control: The orchestration system’s role-based access control (RBAC) lists providing different access privileges to different users', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 480, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e64cd43223a8ab7e92175fb6f7865153', 'text': 'should be integrated with your external IAM solution to provide granular access control based on your global policy. This will ensure that you have a consistent policy applied across your entire network and allow you visibility on the users accessing the orchestration solution.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 481, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '44b2fbb5842e192a98032870fe280024', 'text': '2. Securing interfaces: The orchestration layer will consist of northbound APIs and software interfaces from programmatic or Remote Procedure Call– based protocols (such as NETCONF/RESTCONF) to language bindings such as Erlang, Java, Python, and C, to human-to-machine interfaces, such as a web-user interfaces (UIs), and a set of command-line interfaces (CLIs) that allow straightforward integration into existing business systems and operational tool chains such DevOps Continuous Integration and Deployment (CI/CD) pipeline. To mitigate any MitM threats, these APIs are recommended to be encrypted using TLS—preferably TLS1.3, as it provides better security over TLS 1.2. An API GW or web application firewall (WAF) should be used to mitigate unauthorized use of APIs. If there are any untrusted network interactions on northbound interface (NBI), such as with external third-party developers, then it should be secured using an API GW or WAF.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 481, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '93b2c26ee93bbf8544b65937623e5051', 'text': '3. License and patch management: The multidomain orchestration solution you choose should have web interface, CLI, database, and API implementations that are version aware, so the correct license for the specific version of the 5G component under consideration for orchestration and automation can be checked for any vulnerabilities and patches applied before configuration changes or fresh deployment. This is very critical for CI/CD process as well. This would require integration of the orchestration layer to your license and patch management solution. You should leverage advanced machine learning and artificial intelligence techniques to identify any unpatched software in the slice components and get the relevant patches for necessary updates.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 481, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ec1313caf80d35ce78759bd1cdef4f2', 'text': '4. Validation, compliance, and auditing: The orchestration solution you choose should have built-in support for compliance reporting that will check that all devices and services are configured as expected. It should also show details for any discrepancies, such as a misconfigured VPN on an interface. The report also includes details about all changes that have been performed in the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 481, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e95646121ec893dbfc9d7bda7f9678cf', 'text': 'The orchestration platform should also be able to provision services like VPNs, ACLs, BGP peers, and so on. It should perform network audits to', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 481, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6950b06e6ab3a3aa4bc99b8d0b5c6545', 'text': 'detect if any device configuration has changed with respect to the desired service configuration. The difference can be analyzed by the validation, compliance, and audition solution, and the service can be redeployed if needed. The orchestration platform should not just fire off commands to the network but rather confirm that all changes in the transaction are deployed correctly at the device level by getting a confirmation from the validation, compliance, and audition solution. If at any point of the series, a device or a CNF attribute cannot be changed, the entire transaction should be automatically rolled back. This ensures that there is always a consistent state in your network. The orchestration should follow an ETSI-compliant implementation of NFV orchestration and enable easy integration by offering a flexible interface into which a third-party VNFM or container orchestration can be included.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 482, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bad740c5eefdf6d3c2046fb67ae33373', 'text': '5. End-to-end (E2E) visibility and anomaly detection: The E2E visibility and anomaly detection engine should be integrated with the orchestration layer and provide you with E2E visibility, including the transactions in the encrypted layer. This will ensure that you have visibility of any malicious traffic on the encrypted layer. Some solutions available today provide you this level of visibility without having to decrypt the encrypted layer. This is done by collecting extra bytes from the packet header and understanding the behavior of the client/server handshakes and the selection of the crypto suites during the handshakes. Once such malicious packets are found, the hosts can be automatically put into an isolated quarantine segment of the network to prevent lateral movement of malware. Such implementations in your network would secure the orchestration layer and help you detect and mitigate any malicious behavior.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 482, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2d98b018b42ca2976da1bade62ab2943', 'text': 'Securing the Software-Defined Network (SDN)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 482, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a2676961f7b686f1d923ced952fc085', 'text': 'One of the key challenges you face today are the multiple layers of SDN being planned on for 5G deployments. You might already have a software-only network overlay approach based on host virtualization that offers limited visibility, performance, and scale as well as requires separate management of underlay and overlay network devices and security policies. This requires you to have multiple deployment of SDNs, making the management and operation of the SDN layer a hindrance to the deployment of 5G instead of simplifying it. The traditional security policy model for SDN deployments for 4G is based on a static network topology (bound to network connections, VLANs, network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 482, 'parent\_id': '2d98b018b42ca2976da1bade62ab2943', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c35e0b10ac1604ec943f1fa85d972ce5', 'text': 'interfaces, IP addressing, and so on) and manual service chaining. This model, if followed for 5G deployments, will require policy configuration across multiple security devices (web security, firewalls, IPSs, and IDSs), slows application deployment, and is hard to scale for 5G because applications in 5G are dynamically created, moved, and decommissioned.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 483, 'parent\_id': '2d98b018b42ca2976da1bade62ab2943', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '980a052af9af004de2211dba6ec525e7', 'text': 'You should instead take a deployment approach that addresses the security needs of the 5G CNF, VNF, and hardware-based NFs by using an application- centric, unified, and automated approach to security policies in the on-premises data center and cloud infrastructure that is decoupled from the underlying network topology. The chosen SDN deployment method should also support 5GC NF mobility, offer real-time compliance lifecycle management of the CNFs, and reduce the risk of security breaches by having a robust API security approach. You should follow the concept of application policy, which enables a new open security policy framework that expresses policies using the language of the application rather than network. Policies are defined based on a language that is natural to application owners and not in terms of classical networking constructs like VLANs and IP and MAC addresses. This group policy approach decouples security policy and segmentation from the underlying network topology. An example of such an open policy framework is Open Policy Agent (OPA), which is part of the Cloud-Native Computing Foundation (CNCF) project. OPA is a vendor- and domain-agnostic general-purpose policy engine that helps unify policy enforcement across a wide range of technologies. It gives you the capability to offload and decouple policy decision-making from policy enforcement so that the people responsible for policy can read, write, analyze, version, distribute, and in general manage policy separate from the service itself, without sacrificing availability or performance. It provides a high-level declarative language that lets you specify policy as code and simple APIs to offload policy decision-making from your software. You can include OPA as a library or a daemon to enforce policies in microservices, Kubernetes, CI/CD pipelines, API gateways, and more. Using such an open policy framework, the SDN vendor you choose will be able to apply segmentation on the application, network, and user levels. The SDN vendor should also support all variants of 5G deployments—monoliths, VMs, containers, and cloud- deployed 5G CNFs and applications—along with different 5G services such as 5GC services, 5G support services, 5G N6 services, 5G radio services, and 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 483, 'parent\_id': '2d98b018b42ca2976da1bade62ab2943', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4c7ae6900e265e8bf5a19c7eed17befc', 'text': 'networks, as', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 483, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a5b5a96b20f1b113ea71fa4e6677a5ca', 'text': 'Figure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 483, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '81a1388581e99a0bd2c5344a8298d8b9', 'text': 'Orchest rafor i AP | | SON Fabric SON Controller gg Network Layer PR (- ) cuneasbanaen, .............. ................. UPF MBB ON UPF PC CONAT = loT DI i E : g : i : f : | N— L——— | S—— 5G support 5G Radio 5GC services v services services services services', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 484, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4e598839b9ffb422d64de87f975a6c59', 'text': 'Figure 7-27 Multiple 5G Services Chained with the SDN Network Layer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 484, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c67b79b3d6a89c7e78c8c63af4dd0de2', 'text': 'Securing the Control Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 484, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aa054dd6aa3ad7251c3db4aa76fd2989', 'text': 'Protecting the control plane is important for the SDN solution, as any attack at this layer can cripple the whole SDN network, as discussed previously in the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 484, 'parent\_id': 'c67b79b3d6a89c7e78c8c63af4dd0de2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '52cf755d6a1b40d356ec174948b5d458', 'text': '“Real Scenario Case Study: Threats in the 5G Network Slice, SDN, and Orchestration Deployments and Their Mitigation” section.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 485, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3699cbbe3f612b78d959d19e7522ffc9', 'text': 'Here are some of the common attack vectors for network devices:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 485, 'parent\_id': '52cf755d6a1b40d356ec174948b5d458', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '97dbc06d1f28a69a4915ca71a6ebcace', 'text': '• Denial-of-service (DoS) attacks where excessive traffic is directed at the device interfaces', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 485, 'parent\_id': '52cf755d6a1b40d356ec174948b5d458', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2f51b6999a1bb0cb4b0480ebb2072b2f', 'text': '• Exploiting API vulnerabilities to create disruption, such as slowing down the network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 485, 'parent\_id': '52cf755d6a1b40d356ec174948b5d458', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a7b4d014c6bdff19781ec48715f3dd55', 'text': '• Rerouting packets to malicious servers and creating malicious VNF/CNF for data exfiltration and data hoarding', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 485, 'parent\_id': '52cf755d6a1b40d356ec174948b5d458', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ab9f7618ff1e5bc68e06cfa0a1910dc7', 'text': 'To mitigate these risks, it’s important to have a built-in control plane protection layer. This can be achieved by having multiple layers of built-in SDN attributes, allowing for the specification of parameters for each protocol that can reach the control processor to be rate-limited using a policy engine within the SDN control plane, called Control Plane Policing (CoPP), as shown in Figure 7-28. The policy is applied to all traffic destined to any of the IP addresses of the router or Layer 3 switch. This policy should be deployed on a sub-interface level, thereby providing you with granular protection. CoPP protects the control plane, which ensures network stability, reachability, and packet delivery.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 485, 'parent\_id': '52cf755d6a1b40d356ec174948b5d458', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '700cd75f953cac5b1099123e36975129', 'text': '= API pmmmmm—--—— - SON Fabric ODoS mifganby ~\_—¥ i Control Plane Policing DDoS attack 2 5 on SN G —— S — Control Plane [ —— Network Layer ;o pR— S— P (- rmmmmmabmnnn ) mmmmmmmedeananns, UPF MBB ON UPF PC = { A : g : i : f j S—— L —— [——— L—— | T— 5GC 5G support 5G Radio 5G Data services SG N6/ SGi services Services services services', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 486, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e05f227a9fa6aa99b90137f364356ea4', 'text': 'Figure 7-28 Using CoPP to Secure the Control Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 486, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '97912361e69da28433c261335ca8ca53', 'text': 'As shown in Figure 7-28, CoPP functionalities would protect the SDN control plane layer from DDoS attacks using features such as rate limiting.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 486, 'parent\_id': 'e05f227a9fa6aa99b90137f364356ea4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'de37ac727e3795e373c92eb3c028f342', 'text': 'Securing the Data Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 486, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '790b0d1f69e5282602c14be8cee397cd', 'text': 'The data plane of the SDN layer is susceptible to attacks such as volumetric DDoS attacks. Protection of the SDN data plane should be provided by the Data Plane Policing (DPP) built in to the SDN solution provided by your chosen SDN vendor. DPP can be used to manage bandwidth consumption on the SDN data plane and can be applied to egress traffic, ingress traffic, or both. DPP monitors the data rates for a particular interface. When the data rate exceeds user-configured values, the SDN fabric can either drop the packets, as shown in Figure 7-29, or mark QoS fields in them.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 487, 'parent\_id': 'de37ac727e3795e373c92eb3c028f342', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '1cca80133cdfb45f4bae80acc7de7e6b', 'text': '=1 Pl / pmmmmmm - memmm—-——— N SON Fabric SON Controller DDoS protection on Data 0DoS protection on Data ﬁﬁ [ayer provided by Data layer provided by Data Plane Policing ——————— e —— - ¢ Plane Policing [ ey, - Network Layer Data Plane Policing \\ ..... / — PR— S— P (- rmmmmmabnnnn ...... ........ 9 UPF MBB ON UPF { E : g : i : T j S—— | ——— [——— L——— | T—— 5G support 5G Radio 5GC S5G N6/ SGi 5G Data services services servies services services', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 488, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '72eb4f351246b50f84abdb6c9755b9d7', 'text': 'Figure 7-29 Using DPP to Secure the Data Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 488, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0a007081b1df29da9c18e7c4dbf924ee', 'text': 'As illustrated in Figure 7-29, DDoS attacks from the UPF and IoT data network toward the SDN data plane are guarded against by the SDN solution’s built-in DPP functionality, which checks for the data rate in the ingress and egress of the SDN data plane and drops packets once the threshold is reached/increased or a specific QoS is applied to it.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 488, 'parent\_id': '72eb4f351246b50f84abdb6c9755b9d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e55656c7c39321fdf4b7b487c3130259', 'text': 'Securing the Management Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 489, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '038f08cc2343f87b3c9e8fffcabe2e7e', 'text': 'Securing the management plane should be done using RBAC integration with an MFA mechanism, thereby providing robust access control based on zero- trust principles. This method should be followed for all the components of the 5G deployment, including the network slice management, SDN, automation, and orchestration components.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 489, 'parent\_id': 'e55656c7c39321fdf4b7b487c3130259', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58865f34820f847980636e13b781d853', 'text': 'The selected SDN and orchestration solutions for 5G deployments should have integration with identity providers (IdPs) to enable a use case such as single sign-on (SSO) authentication. Granular access control should be provided with privileges managed per resource using RBAC. The roles implemented should have privileges mapped to them, as explained in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 489, 'parent\_id': 'e55656c7c39321fdf4b7b487c3130259', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b0921ceab951d445e30081430e6b66b9', 'text': '• Account administrator: Full control and management capabilities for the accounts and devices under management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 489, 'parent\_id': 'e55656c7c39321fdf4b7b487c3130259', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ab95d1aeecdb98c3ea5a4f00b1d5d500', 'text': '• Read-only: Read-only visibility into resources under management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 489, 'parent\_id': 'e55656c7c39321fdf4b7b487c3130259', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cb6f97fbe4fb2b486bf09ddcc47f1ecf', 'text': '• Network device technician: Administrative device actions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 489, 'parent\_id': 'e55656c7c39321fdf4b7b487c3130259', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f330d00acf210d249e3bb1e4d370518a', 'text': '• Network device administrator: Administrative device actions including creation and deletion of devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 489, 'parent\_id': 'e55656c7c39321fdf4b7b487c3130259', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd4523eb76ddb5169d7ab02929156e865', 'text': '• Server administrator: Server lifecycle and policy-based management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 489, 'parent\_id': 'e55656c7c39321fdf4b7b487c3130259', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '333c11e1fa24d3c8c555925d447abcb5', 'text': '• User access administrator: User, group, and IdP configuration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 489, 'parent\_id': 'e55656c7c39321fdf4b7b487c3130259', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b5901a99c8dc2ffc5c60e4307507dacf', 'text': 'Figure 7-30 shows the out-of-band control plane, which separates management data from IT production and application data.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 489, 'parent\_id': 'e55656c7c39321fdf4b7b487c3130259', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '16311ee3a2a7da94399f26efc678e1fd', 'text': '- - : Orchestration Orchestration Layer i’ :N—h‘ Management Ly —— I‘i [ ——— User Plane Out-Of-Band Management NBI (AP plane Trafi ‘—l A EmE .- S fmm e ——————— SDN SDN Layer | i{ [ ——— Management S 7 e e e e e e e e e e e e e - Amsmse .- | EMS NMS e st T [y ——— W @-E] B ‘ Seemmeme=. 5G Infrastructure Tmmmmn--', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 490, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e78fc206d3f6befa1eb33e77bf83f427', 'text': 'Figure 7-30 Using OOB Management Plane to Secure Management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 490, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '601ceda4df62812a3be8d85be254303a', 'text': 'As illustrated in Figure 7-30, the use of an out-of-band architecture means that users are not affected if devices are unable to communicate with the SDN controller due to Internet or other service disruptions. Users can still access local management and production networks, and all policies and settings continue to be enforced. In addition, local user authentication is unaffected, and local configuration tools remain available.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 490, 'parent\_id': 'e78fc206d3f6befa1eb33e77bf83f427', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6d8ed35b5454549f2b9c4db49adba09a', 'text': 'You should follow strict policies on data collection. For all data collected, the following additional security practices should be implemented:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 490, 'parent\_id': 'e78fc206d3f6befa1eb33e77bf83f427', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6b3f4b5c07a6bfc56cebd5cd0aa51211', 'text': '• One customer’s data should be kept separate from other customers’ data through virtual data segregation. Data requests by SDN management services should return data specific to the customer account only, and per- customer encryption keys should be used for access.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 490, 'parent\_id': 'e78fc206d3f6befa1eb33e77bf83f427', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0cc15f3cf8b273d0c63b4ed44a29d921', 'text': '• Long-term persistent data should be encrypted at rest.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 490, 'parent\_id': 'e78fc206d3f6befa1eb33e77bf83f427', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5ff1162fdad2744a92426becb596b478', 'text': '• You should also have robust audit logging on the database to understand “who” did “what” and “when.”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 491, 'parent\_id': 'e78fc206d3f6befa1eb33e77bf83f427', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '85880dbde19d0c1ec1ff3e693dc56871', 'text': '• Granular access control policies should be implemented and third-party access to data should not be permitted.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 491, 'parent\_id': 'e78fc206d3f6befa1eb33e77bf83f427', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2886633eba33d24037db2e6c25e489c7', 'text': 'Mitigating Data Exfiltration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 491, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aedd8b0442d670ad4a68509116b11dcc', 'text': 'In 5G deployments, the SDN layer will cater for multiple modes of NF, such as on-premises. Figure 7-31 illustrates one of the methods to mitigate data exfiltration at the SDN layer, and the list that follows explains the data exfiltration mitigation technique using anomaly detection.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 491, 'parent\_id': '2886633eba33d24037db2e6c25e489c7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '52f4bbcfac95e4c5fbe8baab50182e35', 'text': 'Service configuration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 492, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '3b9846f60cf5c8abbc17471f8bb19f40', 'text': 'Service configuration Threat Intel Machine Learning | &Al Elngine Service 1 Senvice 2 Anomaly Detection Engine Nel twork Sl lice B Data Collgction Vulnerabiliy Detection & Patch = management ARTT LA 4 I v NF1, NF 4, NF § Core Network NF 6 Transport SON R EE B Network Access Network I % NB %)) cluster 1 g\\B Cluster2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 492, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a19d59221388db7b7c30a077141ad552', 'text': 'Figure 7-31 End-to-End Visibility and Anomaly Detection Solution', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 492, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd59d206d784d9c73151683adad608007', 'text': '1. Data collection: Data collection should leverage telemetry from devices deployed in the 5G SDN layer such as NetFlow, Internet Protocol Flow', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 492, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cbf6b2734db5e29bbf02b06892a26c68', 'text': 'Information Export (IPFIX), and flow data from the existing infrastructure such as routers, switches, firewalls, endpoints, and other network infrastructure devices. The data collector should also receive and collect telemetry from proxy data sources, which can be analyzed by the cloud- based, multilayered machine learning engine for deep visibility into both network and web traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 493, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '06a71017bef47fe3d1db86c445a0974a', 'text': '2. Anomaly detection: The anomaly detection engine (ADE) for the SDN layer closely monitors the activity of every device and network function on the SDN network. The ADE then creates a baseline of normal behavior across the entire network. In addition, the chosen solution for anomaly detection should include integration with threat intel coupled with the machine learning engine, which has a understanding of known bad behavior. It should apply heuristics that look at various types of traffic behavior, such as scanning, beaconing host, suspected data exfiltration, suspect data hoarding, and so on. These security events should feed into high-level logical alarm categories. The system should then be able to determine what kind of attack might be in play and also tie it to a specific network device within the SDN network layer. These measures would help you identify any attacks or data loss such as any data being exfiltrated out of your infrastructure. Once the risk has been identified, you can take corrective measures to mitigate the risk or let the ADE solution create automated mitigation steps for you. For example, if you identify that the peering switch or router is causing the data exfiltration due to backdoor configurations done by a malicious user or due to malicious code during upgrade, the impacted switch or router can be moved to a segmented network with restricted service. Such segmented networks are also called as quarantine segment or quarantine service network. Moving the impacted devices to quarantine layer will restrict the network access of the devices, thereby mitigating any major impact to the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 493, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8606b8503459ccd54044cc87183de414', 'text': '3. Vulnerability detection and patch management: The data collected can also be used to identify any vulnerabilities within the devices in the SDN layer by co-relating the version of the used software with the CVE IDs of the device vendor. Any device found with vulnerabilities should be indicated, and the exact location of the impacted device should be marked in the topology or in any identifiable format for the security team to act on it. This will help you to establish controls and processes to help identify vulnerabilities within the 5G SDN infrastructure and SDN-dependent components that could be exploited by attackers to gain unauthorized', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 493, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '42cce846a8032dbe21eef7ef5a1ec910', 'text': 'access, disrupt business operations, or steal or leak sensitive data. The patch management system should cater for patching any vulnerabilities identified by the vulnerability management system, thereby providing appropriate protection against threats that could adversely affect the security of the 5G SDN layer or data entrusted on the 5G services. Effective implementation of these controls will create a consistently configured environment that is secure against known vulnerabilities in operating system and application software.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 494, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ed97144aea2021cf804577f1f5a496b7', 'text': 'Securing Network Slices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 494, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4439ba275e4fd28f34698eb7c11b626e', 'text': 'Figure 7-32 illustrates the multilayered security controls implemented to secure the network slices and prevent devices from accessing unauthorized slices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 494, 'parent\_id': 'ed97144aea2021cf804577f1f5a496b7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f04e9edeae48ff9a0cc222eb389f7c5e', 'text': 'PEsEsEsEss s s s ~., ((A)) ONB (DU+CU) e \\ - 0 NFs dedicated for Slice 1 i E e mm————— v Segmentation & ) IOO [solation Monitoring & o ————— Anomaly Slice 1 I Detection RAN - O ; L A E Slice 2 IAM Transport Layer NFs dedicated for Slice 2 i j i', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 494, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1105144c9f7f2dce0d15ec77fb19f63d', 'text': 'Figure 7-32 Securing the Network Slice', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 495, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e673f23e007ce40b7f55ca1ff030dcc', 'text': 'As shown in Figure 7-32, the key techniques to mitigate the risks of unauthorized slice access are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 495, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'de1db1f4e65fefe5a940a34059aff19f', 'text': '1. Identity and Access Management (IAM) security control at the per-slice level', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 495, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '05aecdd5583397304b907afc3fbca159', 'text': '2. Segmentation and isolation between slices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 495, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a666036c027d43d8a9e78b6f6319b0ff', 'text': '3. Data collection and anomaly detection at the slice level', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 495, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '85c6b451753656a2dbe1dc254af6845a', 'text': 'Identity and Access Control', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 495, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '096573480e842a7d9765c69397772558', 'text': 'To prevent unauthorized slice access after the primary authentication, there should be a separate slice-level authentication. This slice-level authentication should be performed by an authentication mechanism separate from the one used for the primary authentication. Figure 7-33 illustrates a slice-level authentication mechanism.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 495, 'parent\_id': '85c6b451753656a2dbe1dc254af6845a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '32e9b2aca0ed35e751e356d6be3a0052', 'text': '! [ S —— - [ ———— ((A)) g\\B (DU +CV) AMF SMF UPF Slice 1 v J l.. RAN Slice 1 Transport Route (-] ar -Slice 2 AMF SMF .. AM Slice 2 Transport Layer UPF Slice 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 496, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e7341a3d57598f7f75084a437fb26d25', 'text': 'Figure 7-33 Multilayered Access Control for Network Slice Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 496, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ca7f2fab8b301896f2ad2a585730ff6c', 'text': 'Figure 7-33 shows one of the methods of ensuring slice-level authentication explained in one of the solutions provided by 3GPP TR 33.813. It is discussed in detail next:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 496, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cee6e8ffc98e8f08fb9def6fcd929a05', 'text': 'a. The UE is authenticated by primary authentication and based on the EAP framework (IETF RFC 3748), where SEAF/AMF takes the role of the authenticator. During the course of authentication, the UE also informs the AMF about its subscription ID and the list of Network Slice Selection Assistance Information (NSSAI) it wants access to. Using the subscription ID, AMF obtains the subscription information for the UE from the UDM to check whether the UE requires further slice-level authentication. During the course of the registration accept message, AMF then sends the UE the list of allowed NSSAI, including the S-NSSAI, which requires slice authentication.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 497, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fa664798e38a1fb2afa2e7079042148c', 'text': 'b. This step will be required based on the subscription information for whether slice authentication is required. If slice-level authentication is not required, then step b is skipped. If slice-level authentication is required based on the list provided by AMF to the UE, then AMF directs the UE to the IAM/AAA server. EA-based authentication is performed between the UE and the specific IAM server or AAA server. In addition, there will be instances in network slice deployments where the IAM server is deployed externally by a consumer of the network slice. Figure 7-34 shows one of the methods of how the slice-level authentication could be accomplished in these deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 497, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ced66e06a170e71e876df3d24e5feddd', 'text': 'A e e m e ——————————— SEAF, DM AUS UDR AMF PCF e S R e S e ~ Primary L e Authentication ¢ | | Secondary | Authentication | AM M -- Enterprise on prem A " ~~---~~.\_\_.. oy = User Plane UPF Enterprise DN ONB ( ) Enterprise Slice Enterprise Slice', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 498, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a9c119513c2364371d75b0dc332eaad8', 'text': 'Enterprise Slice', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 498, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'de843fc0d5bc6174fe8444088193e64a', 'text': 'Figure 7-34 Network Slice Access Control for IAM Deployed at Enterprise Premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 498, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ad380ce2475d064f3ce950b05e7fd2d4', 'text': 'Figure 7-34 illustrates one of the other methods to achieve slice-specific authentication of the device. In this case, the primary authentication is performed by the EAP framework, and the secondary authentication uses the device ID for the enterprise slice-specific authentication. Here, the AMF', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 498, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a627afcb17d67e7bdcfdd6d8919ea8ad', 'text': 'performs the role of the EAP authenticator and communicates with the enterprise on-premises-based IAM solution using RADIUS/HTTPS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 499, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '46d43f0556447917ff1f960f48782203', 'text': 'Segmentation and Isolation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 499, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4ed45c84dcbce46b69cc12c2ac14a120', 'text': 'As you saw in the identity and access control techniques for securing the network slice, there are mechanisms being specified by 3GPP and other optional layered security controls you can use for slice-level authentication. Having slice-level authentication, however, will not secure the slice. This is because the authenticated devices are still prone to device-level vulnerabilities and can launch DDoS attacks on to the slice resources. This can lead to capacity exhaustion in shared transport infrastructure components like transport access and aggregation devices or in shared data center components like shared compute, memory, and storage. Providing the right level of isolation and segmentation requires proper planning and should be applied from the service layer toward the southbound layers, such as orchestration and SDN, and then the 5G infrastructure and 5G NFs, which are deployed in the cloud and on the premises, as shown in Figure 7-35.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 499, 'parent\_id': '46d43f0556447917ff1f960f48782203', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'b60324d886140e82ad5d9fb9e35d696b', 'text': "Slice consumers (Slice reseller / end customer) - - - N Service Layer Multi-Tenant - Service Creation '\\ g g g g g g g g g \\‘ Orchestration & SDN Layer RAN Transport & Aggregation 5GC NFs & DC resources N\\ g Slice 1 \\ Slice 2 Method A N - (Physical isolation) ED &= \\\\:|f||? féizl K ice 2 Slice 1 Method B (Logical isolation) Sice 1 Sice2 T e Slice 1 ce 2 Method C Sloe 1 Sice2 (Hybrid) E 0 ]", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 500, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '20270d7abb0e7504fd324e035ff5d5cb', 'text': 'Figure 7-35 Methods for Isolation in Network Slice Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 500, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7b0a45c4ef71a7e4075125a023820fec', 'text': 'Figure 7-35 shows the isolation at the service management layer and different methods of isolation at the 5G infrastructure and NFs layer. The service management isolation can be provided by using a multitenant platform and granular identity and access control mechanism. The methods of isolation for the 5G infrastructure and NFs are explained as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 501, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7cf8fe8f9f4f562548c1753efae8f145', 'text': '• Service layer isolation: The isolation in this layer is provided by the separation of management by using multitenant solutions where service- level requirements can be defined by the consumer of the slice or you can configure the service-level requirements for the consumer of the slice based on the SLA between you and the slice consumer. If the slice is being utilized by a slice reseller, then the SLA will be between you and the slice reseller. The service layer management will enable you to create end-to-end slice and QoS requirements for the required slice. The multitenant management solution should also provide RBAC, where only people with privilege access can modify the end-to-end slice requirements.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 501, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '15b8ebd449c11ad098cd1b15ec926c5f', 'text': '• Orchestration and SDN layer: Multidomain orchestration and SDN ensure the required configurations of NFs and infrastructure components within a slice. They also cater for slice-level isolation and segmentation via different methods of deployment, such as physically isolated, logically isolated, or a mix of both, are explained in detail next:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 501, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '750b7fed2f1cc6c8335e29a54da33885', 'text': '• Method A: This method shows physically separate slices, such as having separate radio access technologies or separate gNBs deployed for specific slices, separate transport access aggregation devices and fiber for each slice, and separate DC infra, such as separate host hardware and host software for specific slices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 501, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '15aa77c88dce8df500f83e2229941bef', 'text': '• Method B: This method shows logically separate slices, such as using the same radio access technology (RAT) or the same RAT gNBs deployed for all slices, where different slice messages are broadcast with time separation in the air interface, the same transport devices and fiber are used for all slices and logically separated using methods like tagging the slices separately, and using the same host with separation of host resources using VM and security zones, application-based policy control, and microsegmentation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 501, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5a95fb3c5ed08d1fdecad3e9e516fbd5', 'text': '• Method C: This method shows an hybrid approach, where slices are separated logically, such as using the same radio access technology (RAT) or the same RAT gNBs deployed for all slices, where different', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 501, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1c01029be677489e17376339a1d30524', 'text': 'slice messages are broadcasted with time separation in the air interface, the same transport devices and fiber are used for all slices and logically separated using methods like tagging the slices separately, and separate DC infra is used, such as separate host hardware and host software for specific slices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 502, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fee5ead8aa1ea5592442bc631f0acabf', 'text': 'You can have more iterations of the segmentation and isolation methods, but the hybrid options are the most likely used ones. Most of the deployments we are seeing now use a single NF type per host (for example, UPF deployed in one host, with SMF deployed in a separate host).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 502, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '55f936a550effaa09ff5ec917c0bc767', 'text': 'Data Collection and Anomaly Detection', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 502, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '56969d2ec230b7730ed5530aa04cf88f', 'text': 'Once you deploy the slice-level isolation and segmentation, it is important to provide the slice-level visibility and monitoring to detect any anomalies in the slice deployment. This can be achieved by collecting telemetry from network functions and network devices and creating a baseline of normal behavior for each slice. Any variation from this normal behavior can be considered an anomaly and is alerted for further investigation or automated corrective actions planned, as illustrated in Figure 7-36.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 502, 'parent\_id': '55f936a550effaa09ff5ec917c0bc767', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ecfeab24a28d845189603d195183d559', 'text': 'Policy defined \\ Threat for Application Intel RN Anomaly Detection Engine & Corrective action Data Collection Palch management Corrective fic fice action @ (y) Slice 1 Slice 2 Service, m Slice 1 \\B N Orchestration & (DU+Cu) =21 == E : SON Management RAN Slice 1 fice 2 S~ Sios2 i 7 n Slice? =R “— [ ¢ Transport Layer 5GC&DC £', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 503, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eacfd4b24ee5b25c92f8f34492d316ed', 'text': 'Figure 7-36 End-to-End Visibility in Network Slice Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 503, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '16dfbee57d0c79369609a65752f97a04', 'text': 'Figure 7-36 shows you a method of slice-level visibility, and the steps involved are explained in detail in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 503, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6ed49866221c845fcdaf1bd7ced7bb7d', 'text': 'a. Data collection: This step consists of collecting telemetry from various parts of the infrastructure. The data collected includes telemetry such as NetFlow, IPFIX (Internet Protocol Flow Information Export), and other types of flow data from 5G infrastructure such as routers, switches, firewalls, endpoints, proxy data sources, and other network infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 503, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed44522cecfa2c6a2224a10ddb1db131', 'text': 'devices. The 5G infrastructure component will require integration with the legacy network. To prevent any blind spots, it will be necessary to provide visibility into the devices or segments of the switching and routing infrastructure that can’t generate NetFlow natively. This will require solution components in the monitoring layer, such as mirroring port or network tap, and generate telemetry based on the observed traffic. Apart from the network layer visibility, it is important to provide Layer 7 application visibility by gathering application information. This includes data features like RTT (round trip time), SRT (server response time), and retransmissions. The solution you choose for monitoring the network slice layer should support even the largest of network demands. It should perform well in extremely high-speed environments and can protect every part of the network, regardless of size.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 504, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8a9d81073e3e972354a2baf559f3ad7e', 'text': 'b. Anomaly detection and patch management: This step consists of performing analysis on the collected data to perform corrective actions, enhance operational efficiency, and reduce costs by identifying and isolating the root cause of an issue or incident within seconds. The solution you choose for the anomaly detection should provide you with the following capabilities:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 504, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '851967ff2dab9c44ae59812b23d5df68', 'text': '• The solution should be able to detect anomalies within the slice in public cloud, on-premises and hybrid deployment modes.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 504, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '172ed77193aec6b18508e6f7c464c4b2', 'text': '• The solution should be able to monitor all hardware and software components of the slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 504, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0a31b47bf6c0957ada359932a7d8a48a', 'text': '• The solution should be able to consume external threat intel or integrate with a robust threat intelligence feed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 504, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1859b626722211596dad8d046994ba5b', 'text': '• The solution should be using machine learning and a statistical modeling of networks, creating a baseline of normal activity, identifying anomalous traffic, and pinpointing command-and-control communications and data exfiltration within the slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 504, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '61db99adf049c98d98ca18db0b82f397', 'text': '• This layer should have the patch management capability within the anomaly detection system or have a separate patch management solution with the capability of distributing and applying updates to the required network functions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 504, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '06969fc1974966af21b972b093006c66', 'text': '• The patch management should be automated selectively to ensure that critical software is patched only in the maintenance window.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 504, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b043800f34485fc313eac2feaf939b2e', 'text': '• The anomaly detection and monitoring layer should provide graphical views of the current state of the 5G control plane traffic of multiple slices within the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 505, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ccc9d22d603ce4f677b84cdbaed509df', 'text': '• Administrators should be able to construct maps of their network based on any criteria, such as location, function, or virtual environment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 505, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4816836c65a64e9d8160b939509b553e', 'text': '• Other capabilities, such as creating a connection between two groups of hosts, where you can quickly analyze the traffic traveling between them, should be provided by the solution. An example could be visibility on increased signaling requests coming in from specific clusters in the IoT slice might indicate some issues in the cluster or a DDoS attack, with some IoT devices in the cluster being compromised.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 505, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6abf35119495d5e43b8b6e01c32c8588', 'text': '• The solution you choose should provide a full audit trail of all network transactions within a slice and inter-slices. For more effective forensic investigations, it should be able to rapidly detect and prioritize security threats, pinpoint network misuse and suboptimal performance, and manage event response across tall network slices—all from a single, centralized center.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 505, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4233afb352ce4da4169b73a1b56f2eef', 'text': '• The solution should quickly detect suspicious web traffic and/or NetFlow and respond to attempts to establish a presence in your 5G environment and to attacks that are already under way.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 505, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '41c82ecf84debadb71fd063674739fcc', 'text': 'c. Corrective action: This step consists of performing corrective actions based on the analysis performed by the anomaly detection and patch management solutions. The key corrective actions are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 505, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f48ce15a04d6f7931dd2180d37670518', 'text': '• The anomaly detection and patch management solutions should be capable of integrating with the service layer, orchestration layer, SDN layer, and also directly with the slice components. This would give you the flexibility of allowing the corrective actions to be applied to the impacted slice component directly or indirectly, based on your preferred method.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 505, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '93eba227a2bfadc81756c411291cfb01', 'text': '• Send out alerts about any identified anomalous traffic within the slices to your security team.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 505, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bad4b83196207f73008386fb5e64b10b', 'text': '• Quarantine any of the impacted slice components by restricting them to a minimum service slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 505, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cf55ddc01c67939a3922bb5300e4c1ea', 'text': '• Modify attributes such as maximum allowed requests to prevent the CPU exhaustion within devices being attacked in a slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 506, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '41d8a025714135d9f1b6ce334364c2f6', 'text': '• Update the software with patches for devices with known vulnerabilities in multiple slices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 506, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e545f213b3eb6a6915faf07aa2c78ff5', 'text': '• Block any unauthorized traffic escaping the slice network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 506, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '134a78452805d87e6679a0c3c74ee85f', 'text': 'These security controls will help you enhance the slice-level security.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 506, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5741de04946bc9314ce49e65db8bdac6', 'text': 'Securing NSaaS Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 506, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '953ae720fd60be326519e8150458db3f', 'text': 'Network slicing will enable 5G networks to provide tailored services to enterprises that adhere to an SLA established with the 5G network. These tailored services could include network capabilities such as latency, throughout, RAT, bandwidth, latency, reliability, guaranteed/nonguaranteed data rates, security services, and so on. One of the deployment methods is to provide the management capability of configuring the slices to the enterprise itself. This requires multilayered security control to mitigate any threats related to unauthorized slice management access, as illustrated in Figure 7-37.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 506, 'parent\_id': '5741de04946bc9314ce49e65db8bdac6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'bcf8ddebf999cbd5c3035ce587537553', 'text': 'Service Layer pemmdecccccccc e e cc e ————. - - - .- Management | | " A :, : - - Enterprise Slice - - . \' Secure API Service operations & SLA = : T Management e \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Voo messssssssssssssaa—. P TTIIII I TS /’ | - Ent@% Slice (y) | : Govt Defense Slice g E (U == ] | 25 \\', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 507, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da598b7433cb1f43be2e62bde3bda1dd', 'text': 'Figure 7-37 Method to Mitigate Unauthorized Access to Slice Management Layer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 507, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e61d75ade07a6445369e1c75399b9d58', 'text': 'This section will take you through the key security controls to mitigate unauthorized slice management access. The key security controls are described in the sections that follow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 508, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4cb8b5344e06cef90894186e4ba81db1', 'text': '1. Granular Identity and Access Management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 508, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '28a4061e6ed4fe59b0dc7120bb10f024', 'text': 'It is recommended to use the zero-trust principle-based granular access control to provide the right level of access control to the admin of the slice provider and the slice consumer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 508, 'parent\_id': '4cb8b5344e06cef90894186e4ba81db1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36448d9f678cbc106e17945f463b5525', 'text': 'Figure 7-38 illustrates the key security controls required for ensuring granular Identity and Access Management and is explained in detail in the list that follows.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 508, 'parent\_id': '4cb8b5344e06cef90894186e4ba81db1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a8f3dbe4c04a07ecdc378a41266df05a', 'text': '’ Slice Provider Admin . Slice Consumer Admin B I el |AM Granular - @ 0 ) a1 security controls Primary Secure internet Secondary RBAC - Role based E Authentication access Authentication access control R L L L L L T N E Service Layer - e e e e e ey ,---------- I I :, Lo = ﬁ---------l e e e e e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 509, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dc07efba37ef5d1f8422afb0a4e3bad1', 'text': '|AM Granular security controls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 509, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'deb064d85a36c863203a0e0a23efdead', 'text': 'Figure 7-38 Multilayered Access Controls to Mitigate Unauthorized Access to Slice Management Layer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 509, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '62062abbd52c1d73026385e46b953876', 'text': '• Based on the zero-trust principles, the access to the network slice service layer should be dynamic and be determined by various conditions such as the software version and type of the device, network location, time/day of the request, and historical behavior of the requester, such as previously observed behavior and credentials. This includes the use of multifactor authentication to access the NSaaS management layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 509, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '235c7b5dca07b3182d65c9b3460f93a5', 'text': '• Slice-specific authentication and authorization policies should be defined such that each is mapped to the allocated slices and can operate only in authorized slices. This function can be performed by using an identity management system that is responsible for creating, storing, and managing user accounts and identity records.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 510, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '293e48977d22ce376237805aa6f6aa60', 'text': '• As shown in Figure 7-38, RBAC is also implemented to ensure that different users from the same slice can have varying levels of access, as per their roles. For example, the slice admin can modify the attributes of the slice, whereas a non-admin user will have read-only access to the management system.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 510, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dea83eec007462c12f88e0a57467969e', 'text': '• Based on the zero-trust principles, the access to the network slice service layer should be dynamic and determined by various conditions, such as the software version and type of the device, network location, time/day of the request, and historical behavior of the requester, such as previously observed behavior and credentials.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 510, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0b714420693dc589995f9b68aeac32d1', 'text': '2. Segmentation and Monitoring of the Management Layer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 510, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '94cee5de7cd938403b83b0f5d95af2e6', 'text': 'Segmentation of the NSaaS layer should also include the NSaaS management access policy, which is microsegmented per NSaaS slice management. The idea behind using microsegmentation is to divide the data center into small zones that can then be effectively managed. This will allow granular security control of the users accessing the NSaaS management plane. Segmentation is also critical at the SDN layer for the NSaaS services.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 510, 'parent\_id': '0b714420693dc589995f9b68aeac32d1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b681c04bc52ad439942ce6edb282bfa6', 'text': 'The out-of-band control plane in the SDN platform you choose must separate management data from application data. Management data, such as configuration and monitoring information and statistics, must be directed from the 5G devices within all slices to the SDN controller. Application data from all the network functions should be sent directly to its destination on data network configured for the respective slices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 510, 'parent\_id': '0b714420693dc589995f9b68aeac32d1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '80665e01b98fbd6dc131271416a93d1c', 'text': 'The use of an out-of-band architecture provides resiliency for the users. It means that users are not affected if devices are unable to communicate with the SDN controller due to intentional or unintentional service disruptions. Users can still access local management and production networks, and all policies and settings continue to be enforced. In addition, local user authentication is unaffected, and local configuration tools for the 5G infrastructure remain available.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 510, 'parent\_id': '0b714420693dc589995f9b68aeac32d1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5f3819c2e436dc5378ae3c7342c761dd', 'text': 'Figure 7-39 illustrates the microsegmentation layer for policy mapping and enforcement for the users accessing the NSaaS management layer, as further described in the list that follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 511, 'parent\_id': '0b714420693dc589995f9b68aeac32d1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'df26f43f6944a3c1d5c017e3ba564907', 'text': '. Slice Provider Admin ‘ Slice Consumer Admin D 4 = Q@ L, L Global Policy i Primary Secure internet Secondary RBAC - Role based Engine Authentication access aceess control (- Authentication Custom Policy per NSaa$ slice Granular IAM security controls A U S S —— R R e Policy enforcer for Micro- Palicy per NSaaS Palicy per NSaaS segmented policy per slice management - - slice management NSaaS slice management Management Management . . Govt Defense Slice :, Enterprise Slice Syl R Sy —————— | Senvice Creation NSaaS Service Layer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 511, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e81e298280478a93f11c9b440357fdfb', 'text': 'Figure 7-39 Microsegmentation Layer for Policy Mapping and Enforcement at the Application Layer', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 511, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd048ee2f80f521e4b49bd46180bf097e', 'text': 'a. Global Policy Engine: The Global Policy Engine should be able to take policy inputs from multiple sources, including manual and automated components. This will improve your policy engine for the right decision, such as granting, denying, or revoking access to the management of the NSaaS slice. The global policy engine should also be able to log the action taken by it for each of the request', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 512, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b37e955e81e537f17813e62f25a22f26', 'text': 'b. Policy per NSaaS slice management: This layer is responsible for dynamically granting access to individual requests toward the NSaaS slice management layer per slice. When the management is deployed as a virtual machine or a container, the policy should be applied at the application layer so that the policy sticks to the virtual instance whether deployed on the cloud or on the premises.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 512, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2edec9396900075ee0be4ccb64565d2c', 'text': '3. Connection Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 512, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5a562d9034eeadcc2b2ac6d7a7b873dd', 'text': 'This section will take you through the different methods to secure the API communication for NSaaS and network slice components. All APIs in the 5G service, SDN, and orchestration layers should be secured using TLS, as shown in Figure 7-40.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 512, 'parent\_id': '2edec9396900075ee0be4ccb64565d2c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '0e7f83b8aad530c432914a4c6dcf8bec', 'text': 'Service Layer ‘ | HTTPS e II [P —— B . | | (y) Ent@% Slice - | Govt Defene Slice E gN\\B ~ [ Transport \\‘(DU +CU) e mssss s s e .-', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 513, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '81a7ccc3a80d4e606bf91e8940eb7f71', 'text': 'gN\\B +CU)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 513, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e61e79f0a01f0621ca7cddcb7123adb', 'text': 'Figure 7-40 Secure API Connections', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 513, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '62ead9dcc089eeafcacaa339db9055c9', 'text': 'As shown in Figure 7-40, all management communications and traffic flow between the different layers should be secured. Because APIs would be used mostly in the exchange of data, encrypting the traffic using Transport Layer Security (TLS) is recommended.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 514, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1627faaa23ef45e70edb61c3d216aec3', 'text': 'Figure 7-41 illustrates encryption of the API communication between the SDN controller and the on-premises/cloud components using HTTPS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 514, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6565e023f0cd98e59cc76491207ca53b', 'text': 'As shown in the figure, all data exchanged between devices within the slices and the SDN controller should use industry-standard encryption and security protocols. Connected devices should use TLS with restricted ciphers and HTTPS on the standard HTTPS port 443. All data sent to the SDN controller should be encrypted using the Advanced Encryption Standard (AES) with a 256-bit, randomly generated key that is distributed with a public-key mechanism to prevent man-in-the-middle attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 514, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '87ccead93851eaaddb40fd520ee2250e', 'text': 'SON Contoler ‘ HTTPS HTTPS ¥——aAa Attacker —— — — — —\_— \\ o Wl | === 5GC VM 5GC Container o deployment deployment — — — — — 5GC NFs On-premises deployment 5GC NFs cloud deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 515, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'bb516653956a5c7359d8a1b1de900a9f', 'text': 'Figure 7-41 Secured API Connections Mitigating MitM Attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 515, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b413e547c778cf4e5848a12296d180ad', 'text': 'In addition, every device connecting to the portal should be authenticated with a cryptographic token so that only legitimate devices can be managed, thus closing a potential Trojan horse attack vector.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 515, 'parent\_id': 'bb516653956a5c7359d8a1b1de900a9f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36fd4018d599d4efc88608e5cc92296d', 'text': 'All connections should be initiated from the device. Thus, firewalls can block all incoming connection requests. Only HTTPS port 443 needs to be enabled for outbound connections. As a result, firewalls do not need any other special configuration to enable SDN controller connectivity. All network devices and', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 515, 'parent\_id': 'bb516653956a5c7359d8a1b1de900a9f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eb975acc41d6956a11fe27b49be0a0cc', 'text': 'network functions can be configured to use HTTPS proxy servers to add an additional layer of security through indirection.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 516, 'parent\_id': 'bb516653956a5c7359d8a1b1de900a9f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9099bbff74a6f0346dcd4aab59e644ef', 'text': '4. Secure API', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 516, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '49e369e8279c3f056112a80080414513', 'text': 'A majority of the communications in the 5G NSaaS infrastructure is based on APIs. This includes the API-based communications between the 5G network functions in the SBA architecture defined for 5G, northbound interfaces (NBIs) from the programmable transport devices toward the SDN controller, NBIs from the SDN controller toward the orchestration layer, and NBIs from the orchestration layer toward the NSaaS service layer. The external integrations, such as from the slice consumer and the slice reseller, are also based on the API calls. This makes APIs one of the critical components in NSaaS deployments. API connection security using encrypted API communication was covered in the section “3. Connection Security,” earlier in this chapter. Figure 7-42 illustrates other API security methods to safeguard NSaaS deployments from attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 516, 'parent\_id': '9099bbff74a6f0346dcd4aab59e644ef', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'e7edcefbc3f9598f184b6ee2f25cb466', 'text': 'e e e e Encrypted Senvice m M Traffic API GW | WAF Analysis il ------------- .\_---\_-\_-\_- =N = External Malicious | Application = Application Server e Ll / Z % /» 7 > . Attacker N | = @ PSS Slice 2 pmmmsseeneabony Transpon Route 1 00 (A) Transport Route 2 Slice 1 = | Transport ! } G0 g\\B e Nesnsssssssssanas (DU+CU', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 517, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ec05a192adcf8c819fe442842925f362', 'text': 'Figure 7-42 API Security Methods to Secure the NSaaS Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 517, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fb40bca6b82347d1463be4a3aa0d1180', 'text': 'The key security controls for NSaaS deployments are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 517, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f253380e4695dd0267e9848474d7c480', 'text': 'Step a. API GW/WAF: Any API calls originating from external network or from untrusted zone should be inspected by the API gateway (API GW) or the web application firewall (WAF). Here are some of the key capabilities required at this layer:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 517, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '439d18eca32a58ed43bba7c31bae4d09', 'text': '• Authentication: Improper or broken authentication within API communication is widespread due to the design and implementation of most identity and access controls in API calls. Attackers can detect broken authentication using manual means and exploit it using automated tools with password lists and dictionary attacks. To secure your network from these kinds of attacks, the following steps should be considered:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 518, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c93c152910ba18456e6e1d303ba1295f', 'text': '• You should ensure registration, credential recovery, and API servers are hardened and updated with latest patches.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 518, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e2a23fc67a304edb39653597a2f2acdb', 'text': '• You should apply rate limits and thresholds on API requests, such as repeated requests for login, to mitigate DDoS attacks. You should log all failures and alert administrators when brute force and other attacks are detected. Use a server-side session manager that generates a new random session ID with high entropy after login. Session IDs should not be in the URL; instead, they should be securely stored and invalidated after logout, idle, and absolute timeouts.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 518, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9481f1c3ef95ac7b581af6046a74d958', 'text': '• You should use JSON Web Tokens (JWTs) to secure the REST API. JWTs are URL-safe JSON-based security tokens that contain a set of claims that can be signed and/or encrypted. JWTs are being widely used and deployed as a simple security token format in numerous protocols and applications, both in the area of digital identity and in other application areas. The most common use case for JWTs is to use them as access tokens and ID tokens in OAuth and OpenID Connect flows.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 518, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b6e6073904ec7847c19226fc5a2d35b4', 'text': '• You should deploy MFA to prevent unauthorized users and devices access to slices. Do not ship or deploy with any default credentials, particularly for admin users.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 518, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '55aef5289ebe2cafd1ecd402536c8ff8', 'text': '• Authorization: APIs are also prone to weak or broken authorization due to lack of proper functional testing by the application developers. This might result in the MEC applications used by the NSaaS services being exploited, leading to unauthorized access to slice resources by illegitimate users.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 518, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '79d9ef186f45b55b755483e37351accf', 'text': '• To mitigate such unauthorized access, you should conduct regular audits and implement authorization checks for users. The global policy engine should also be audited to check user policies and hierarchy.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 518, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6f959f778d4b3f5d4986767cb9182a39', 'text': '• The authorization should be implemented on both the client side and the server side. Just having client-slide authorization, such as relying on client IDs sent from client, is not recommended.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 519, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8306b2ecb0e8d3856658f6a43883d582', 'text': '• Each time you have a request from a client or a user, the authorization policy for accessing the database should be checked.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 519, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cb87ad5ff655bfb8570a1f6af2705ed1', 'text': '• Input validation: Input validation is another area that should be carefully planned. 5G introduces openness to your network by allowing third-party software and application integrations with your 5G network. For NSaaS deployments, this means having the 5G slice integration with the required third-party applications or having the third-party applications deployed within the slice for fulfilling the use case for the network slice reseller or network slice consumer. Input validation prevents malformed data from entering your 5G network. In such deployment scenarios, it is difficult to detect a malicious user who is trying to attack software applications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 519, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '37b39b735820d72cbfde29141f14f7d8', 'text': '• To mitigate such attacks, you should have a security control to check and validate all input entered into a system, such as validating the user input for any unexpected attribute values. For example, many organizations use automatic binding of HTTP request attributes to server-side objects. This can allow an attacker to update server-side objects that were not meant to be modified. The attacker can possibly modify their access control level or circumvent the intended business logic of the application with this feature.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 519, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ea59382565c39943d7418f609aa0c24d', 'text': '• To prevent such attacks, you should avoid automatically binding inputs directly and put a rule in place that allows only specific fields or attributes that are allowed to be auto-bound.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 519, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2102a40a135ad2083710470ccd98aea8', 'text': '• Rate limiting: APIs do not impose any limitations on the size or number of resources that can be requested by the client/user. Depending on the type of API attack, it could not only degrade API server performance, leading to denial of service (DoS), but also could leave the door open to authentication flaws such as brute force. You might think that the brute- force attacks could be mitigated by locking accounts after a limited set of attempts, but the attacker would use this exact method against you.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 519, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd64f88c79b3b0205d0e07620a26804f3', 'text': '• For example, consider a brute-force attack in the NSaaS service management layer, where the slice configuration parameters are set. An attacker might perform a brute-force attack on all the accounts', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 519, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c1b7ebfbef2fd59a00fb3de10212ac94', 'text': 'being used for the NSaaS slice resellers or slice consumers and intentionally lock all of them out.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 520, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '10dc64db587da857141b3b90b1cd1f1e', 'text': '• It is recommended to design your security architecture in such a way that if the rate-limiting solution fails or is unreachable, your service should fail open and try to serve all requests for critical services required by the NSaaS slices. The clients should then go through the multilayered access control mechanisms before being allowed to access the system, including the input and output validations. Failing closed leads to a complete outage, versus failing open, which leads to a degraded condition.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 520, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d8b2cee768d9fa127036c252298985a', 'text': '• Configuration audit: Having a proper validation process will ensure that the data being sent to the API is restricted and that only the required data is being sent. This will reduce the risk in sending too much information over the API for the attacker to gather more information and then plan an attack on your infrastructure. To enhance the security of the API, the following configuration audits can be performed:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 520, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6dbb02c6e38c4d7144e9c8959b09d460', 'text': '• Define and enforce all API response payload schemas, including error responses, to prevent more information being passed during error exception, which might allow attackers to have more information about the type of software and web servers being used for the NSaaS service layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 520, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b58cfe13f248dd2d4dc6b2a0cec5f2b4', 'text': '• A repeatable hardening process leading to fast and easy deployment of a properly locked-down environment for any impacted NSaaS slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 520, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '79c0f363fcdaf0774890ef558104be1f', 'text': '• Continuous review and update configurations across the entire API stack for slice resellers and slice consumers, such as orchestration files, API components, and cloud services.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 520, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '469c24d83a27fa01347262a52d5e938e', 'text': '• An automated audit process to continuously assess the effectiveness of the configuration and settings in all environments such as on- premises and public cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 520, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5c95972f62864a34cb31d60250e095f6', 'text': 'Step b. Analyzing encrypted traffic: Encrypting API traffic in 5G networks is recommended to prevent MitM attacks in the NSaaS service layer, orchestration, SDN and 5G service-based architecture deployments. But encrypted traffic also creates an additional challenge for security teams. They now have to address a massive influx of traffic that they cannot look inside without decryption technology. The hackers have quickly learned to use data encryption to their benefit to conceal delivery, command-and-', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 520, 'parent\_id': 'ec05a192adcf8c819fe442842925f362', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8af2cf2fb5ecb1b3d1bace3872ee16f7', 'text': 'control activity, as well as data exfiltration. Thanks to encryption, they can now break into the network and stay undetected for months. This is critical for NSaaS deployments, as there might be a slice for critical infrastructure deployments that needs to be protected from such attacks. To address the challenges of data encryption, it is important to identify any malicious packets in the encrypted traffic. The most widely used method for this purpose is to use SSL decryption engines to decrypt the encrypted packets and then run anti-malware or HTTP inspections. However, this requires multiple encrypted traffic to be decrypted, thereby breaking the security posture of your network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 521, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '83dcd1e32353c480dde041a198e679ce', 'text': 'Another way of addressing this challenge is to use solutions available today that identify malware within an encrypted layer without having to decrypt it. This is achieved by solutions that collect the packet flow from multiple network devices and then look into the header of the packets to identify necessary information such as cipher suites being used, cipher suites being chosen by the server, and so on. This information is then analyzed by ML and AI engines along with threat intelligence feeds to determine any malware within the encrypted packets. The key functionalities that should be supported by the encrypted traffic analytics solution are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 521, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '558c302d33f123c4f8277547b514d267', 'text': '• The chosen solution should provide insight into threats in encrypted traffic and contextual threat intelligence with real-time analysis correlated with user and device information.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 521, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '807e5aac25af0f8daca623453561d1f3', 'text': '• There should not be any need to decrypt the traffic. Analysis should be performed without the need of decrypting and then re-encrypting the packets.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 521, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '313d524f7add9de3ce41cf6d511c8e0f', 'text': '• The solution should be able to provide cryptographic assessment, such as compliance with cryptographic protocols and visibility into and knowledge of what is being encrypted and what is not being encrypted on your 5G network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 521, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a6a496216076c7af194248d758f8376d', 'text': '• There should be quick identification and isolation of infected devices and users (faster time to response).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 521, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '416a1e52e62ea3d34c2b04109c84e7f6', 'text': '• The solution should be able to integrate with your existing security information and event management (SIEM) solutions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 521, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c199130e80298c99b090279cfd6f19b1', 'text': 'Real Scenario Case Study: Threats in the 5G Network Slice, SDN, and Orchestration Deployments and Their Mitigation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 522, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9f5932e56280ed0bcc7c8ab4c694f841', 'text': 'The previous sections described the threats and mitigation techniques for specific areas of concern while deploying a 5G network slice that is enabled by the SDN and orchestration layers. This section focuses on a multidomain attack and discusses methods to deploy security controls at different parts of the infrastructure to mitigate attacks in a real-life environment. Although the 5G network slice was not widely deployed at the time of writing this book, this section is based on real-life attacks in similar environments or proof of concepts and lab tests done by various customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 522, 'parent\_id': 'c199130e80298c99b090279cfd6f19b1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6784174f701d6b82d474998b64f1239f', 'text': 'To explain the attack scenarios, Figure 7-43 shows an example of the V2X deployment as a reference for this section.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 522, 'parent\_id': 'c199130e80298c99b090279cfd6f19b1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '6f6f5250312654ea270278c012b025c9', 'text': 'Common 5G NFs for all lices - B RAN Layer Edge Layer Slice #1b- V2X Siice 2 . Slice 1- V2X Slice i Common PCF UPF 86 Common AMF SMF MEC Infernet / Apps Slioe #1a - V2X Slice Appln Slice 2 - MBB Slice NRF PCF UPF ) UPF 3 Internet 10 SMF MEC Slice #2- BB Siice Appln Slice 3- loT Siice MEC Internet / Apps AVF Appln UPF @ 3 PCF UPF Slice #3- loT Slice', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 523, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f4221e85f01e315946724a247ca7f236', 'text': 'Figure 7-43 Example of the V2X deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 523, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cafc1364fbbfaa7a84315891a4af09e1', 'text': 'The 3GPP and non-3GPP network functions are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 523, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9613ed05dd4ddbc0eb77c667fc688ea8', 'text': '• AMF (Access and Mobility Function): Responsible for handling all connections and mobility-related tasks for the UE', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 523, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2e76acddfb9dafeb3578579f8d18aa1', 'text': '• AUSF (Authentication Server Function): Manages UE authentication', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 523, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '22cf06541308f6945296a6134cf86236', 'text': '• NRF (Network Repository Function): Centralized repository for all the 5G network functions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 524, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd05eb2374e66f4665f781d33e506e22e', 'text': '• NSSF (Network Slicing Selection Function): Helps in selecting the network slice available for the service requested by the user in the 5G environment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 524, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f7e1e2e15252945ff1c11a3e397c1b16', 'text': '• SMF (Session Management Function): Responsible for managing session context with the User Plane Function (UPF) and creating, updating, and removing Protocol Data Unit (PDU) sessions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 524, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2390bddfed319e553ac30b2873016e8e', 'text': '• PCF (Policy Control Function): Provides policy rules to control plane functions to enforce them', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 524, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b715f451787e23530176a24a1e25c013', 'text': '• MEC Application (Multi-access Edge Compute Applications): Application created by third-party developers deployed on the edge network components', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 524, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ea0c0a9ecb0503ca51a5b4e19593f3ea', 'text': '• UDM (Unified Data Management): Manages data for access authorization, user registration, and data network profiles', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 524, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9d3739ebd0dccf22eca63567323f11db', 'text': '• UPF (User Plane Function): Responsible for packet routing and forwarding, packet inspection, QoS handling, and external PDU session for interconnecting data networks (DNs) in the 5G architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 524, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da05e451fb753ddc0ad5a6c721a4420c', 'text': 'Figure 7-43 shows the logical design of the 5G deployment for the multiple network slices. All the slices share common NSSF, AUSF, and UDM 3GPP network functions. Each slice has the following dedicated components:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 524, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '918ec0e912904c8b5c95b78b8f71d03b', 'text': '• Slice 1: Slice 1a and 1b in Figure 7-43 cater for vehicle-to-everything (V2X) use cases and have shared AMF and NRF network functions. This slice has a dedicated SMF, PCF, UPF, and 3GPP-based network functions. It also has a dedicated third-party MEC application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 524, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '83d9fd82faf3e9e6142455b7ef9bee3f', 'text': '• Slice 2: Caters for mobile broadband (MBB) use cases. It has dedicated AMF, SMF, NRF, PCF, UPF, and 3GPP-based network functions. It also has a dedicated third-party MEC application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 524, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b1c7ad7f15f9171e49324fb7a4e8fff0', 'text': '• Slice 3: Caters for Internet of Things (IoT) use cases. It has dedicated AMF, SMF, NRF, PCF, UPF, and 3GPP-based network functions. It also has a dedicated third-party MEC application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 524, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '822cb337ec6be837271081d3905856e4', 'text': 'To understand the threats in real-life scenarios, let’s look at how the slices are deployed (or are planned to be deployed) in actual 5G networks by service', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 524, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4ec0eed809a0cd13fb0d1f717613ed11', 'text': 'providers. Figure 7-44 shows the DC design of the 5G deployment for the multiple network slices in a real-life scenario.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 525, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '8c0ab9916c6e73d1d24dd7c7868794bd', 'text': 'Internet ToR ToR switches switches Centralized 5GC UPF UPF UPF NRF NRF NRF SMF SMF SMF 3 party 3¢ party 39 party Slice Slice Slice Appin Appin Appln Slice Slice Slice Sice Slice Slice Slice 1 Slice2 Slice 3 flan oon Bon L m B M = = = - ﬁ', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 525, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3c79b9426a2397da56d6fd6ff365cb4d', 'text': 'Figure 7-44 Example of the Actual Network NF Deployments per Slice', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 525, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a76aa90492bb043b2589872f6a973127', 'text': 'Figure 7-44 shows an example of on-premises network slice configuration for a 5G network. The same logic can be used when the 5G components are deployed in the public cloud, but the majority of the proof of concepts or deployments for network slices are initially on-premises.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 525, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ff4a248a3046e071f37cd410bcb9c7a', 'text': 'To allow scalability and flexibility with the different orchestration solutions, the NFs are clubbed together in an x86 server. For example, Figure 7-44 shows you third-party applications together in one x86 server, and UPFs for all slices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 525, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8c657d02dbd1dd79700a728c3b3c8ed4', 'text': 'deployed together in another x86 server. This applies for all the other 3GPP NFs. Depending on the use case, all the 3GPP and non-3GPP NFs can be deployed in the same DC or distributed in multiple DCs. If the DCs are distributed, a back haul would be required between the edge DC and the centralized DC. If the DCs are not distributed, then the top of the rack (ToR) switches would be interconnected to allow user plane and control plane traffic flows. In real life, there will be multiple x86 servers handling a single NF; for example, for testing all three slices in a cluster, you will require anywhere from three to four x86 servers only for UPF NFs, depending on the traffic volume and throughput for the test cluster. Real-life deployments to cater for your entire subscriber base are a whole different scenario with multiple servers being dedicated to each NF.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 526, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0e6c18c6a751a332d27f8ebe24b8f2b8', 'text': 'Threats: Case Study', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 526, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '31ef173499a2dd443666492dcca75f14', 'text': 'Let’s look at the threat surfaces in these real-life scenario deployments. Figure 7-45 illustrates one of the threat vectors.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 526, 'parent\_id': '0e6c18c6a751a332d27f8ebe24b8f2b8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '3c4fb0aebef0bdffe3237b019793f03c', 'text': 'Common 5G NFs for all slices RAN Layer Edge Layer PCF Slioe #1b - V2X Slce 2 Slice 1 - V2X Slice i Common NRF PCF UPF e Common AMF SMF MEC Slice #1a - V2X Slice Appin Infernet / Apps Slig 2 MBB Slice NRF PCF UPF AMF UPF Internet If SMF MEC Slig #2 - MBB Siice Appln Slice 3- oT Siice MEC 0 Appln UPF A Intemet / Apps AMF Attacker SMF PCF a:r — UPF Slice #3- loT Slice', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 527, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0166af1d97d4f1ead10f43c62e78176b', 'text': 'Figure 7-45 Attacker Exploiting the Weak API Implementation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 527, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f77cbada7e5c0ed1e138f7ea941af31c', 'text': 'In this scenario, an attacker is exploiting the weak API implementation. One of the key attack vectors is the privilege escalation attack. Privilege escalation is a type of attack used to obtain unauthorized access to systems by exploiting a bug, design flaws in API implementation, and a misconfiguration in an application or operating system. To make the scenario a bit clearer, Figure 7-46 shows the actual physical deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 527, 'parent\_id': '0166af1d97d4f1ead10f43c62e78176b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '9126f135519b506f11ad85ada8d7a8a1', 'text': ') Attacker Internet ToR ToR switches switches Backhaul Centralized MEC 5GC 3!‘6 pa 3% party 3¢ party UPF UPF UPF NRF NRF NRF SVF SMF SMF Slice Slice Slice Sice Slice Slice Sice Slice Slice Appln Appln Appln Slice 1 Slice2 Slice 3 L 0 R GO m B M = = = - ﬁ', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 528, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '23ee8fb56fe9720767f381402085bc2b', 'text': 'Figure 7-46 Illustration of Attack in Real-life Network Slice NF Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 528, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f5dfc0156446a852d52bbb7c48a9e2d6', 'text': 'Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 528, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1f15741796df4a6fc35c5b19c67abe3d', 'text': 'Once the IoT slice MEC application vulnerability and misconfiguration are exploited, the attacker proceeds to perform multiple attacks. Figure 7-47 illustrates one of the risk vectors, as explained further in the list that follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 528, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '4df638960c058f00009310f6df4a3b67', 'text': 'Common 5G NFs for all slices RAN Layer Edge Layer PCF Sliog #1b - V2X Slce 2 Common PCF UPF Ea i w Common It AMF 3 MEC Appin Internet / Apps Slice #1a - V2X Slice 3 PCF UPF UPF AMF il SMF MEC Internet Slice #2- BB Siice Appln MEC Appln UPF IE SMF PCF UPF Slice #3 - loT Sice labasaat | Aana', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 529, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '78441af50a4a27464b3f9b6f4b0e34ad', 'text': 'labasaat | Aana', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 529, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '01077d01ebd42e9045e0a877a219dada', 'text': 'Figure 7-47 Illustration of IOT Application Infecting the IoT Devices with Malware', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 529, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '01db7f02164ce830a773dad48c27b2de', 'text': 'Step 1. The attacker exploits the vulnerabilities and misconfigurations in the API and web server deployment to deploy malicious code in the IoT devices. Once the IoT devices are under the attacker’s control, the attacker could choose to perform a DDoS attack on the service provider infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 529, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dd84e132dd41c0e34c721e2c5bcb1e68', 'text': 'Figure 7-48 illustrates the attacker spreading the malicious code in other slices using the privilege escalation attack in the shared host infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 530, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '2805bb26b6622ad3ca2cb6fbe5e3c78a', 'text': 'Common 5G NFs for al sices RAN Layer Edge Layer A PCF Slioe #1b - V2X St Common NRF PCF UPF Eﬂ i Common AMF SMF MEC Slice #1a - V2X Slice Appln Internet / Apps NRF PCF UPF UPF AMF MEC Internet il Sliog #2- MBB Siice SMF Appln NRF MEC UPF Internet / Apps AMF Appln lﬁ SMF PCF UPF Slice #3- loT Slice Internet / Anns', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 530, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '72b9e95b620f7e50a98d91eaf2991a51', 'text': 'Figure 7-48 Illustration of Malware Spreading to Other Slices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 530, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '04e2e4d41c004f0a604aeb4cada34f94', 'text': 'Step 2. Once the attacker exploits the MEC application for the IoT slice, one of the attack vectors is to infiltrate other MEC applications dedicated to', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 530, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ceb1aacd7f4afc598a5d0cac5b71cbd6', 'text': 'MBB and V2X slices, as indicated in Figure 7-48.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 531, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3861ff18721fde27924a9ad7aa94780d', 'text': 'To clarify the attack vector better, the attack is shown in the physical design in Figure 7-49.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 531, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '9b456f06b9cb15107998758aa8c68c54', 'text': '0 Attacker Internet ToR ToR switches swifches Centralized MEC Backhaul 6GC 3[0 pa UPF UPF UPF NRF NRF NRF SVF SMF SMF 3 party 3¢ party Slice Slice Slice Slice Slice Slice Appln Appln Appln Siice Slice Slice Slice 1 Slice? Slice 3 2 L el A ik waty el - — o— [N o — [« — | (] \\J = = = Privilege escalation attack through shared host', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 531, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2472e273d8f8f78a00e9e2106f1c00d7', 'text': 'Privilege escalation attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 531, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '64b608d156173f303cc0f14945f34b6d', 'text': 'through shared host', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 531, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c26cb179bde5db0cce8d227294924938', 'text': 'Figure 7-49 Illustration of the Actual Process of Malware Spreading to Other Slices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 531, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '57918f02f210b7df416797f859416e19', 'text': 'Figure 7-50 illustrates the steps the attacker performs to disrupt services to the critical V2X slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 531, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c5ffe3cbd926b4ec79c612b59b2f1e61', 'text': 'Common 5G NFs for all sices 2 RAN Layer Edge Layer 19 MEC Slice #1b- V2X Siice Appln Common i NRF PCF UPF Lo AMF SWF 9 MEC Internet / Apps Slice #1a - V2X Slie Appln NRF PCF UPF ) UPF AMF Internet il SMF MEC Slice #2- MBB Siice Appln MEC 3 UPF Internet / Apps AMF Appln lﬁ SMF PCF UPF Slice #3- o Sice', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 532, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2abec221a6ed70c88ca07e7ca847d96c', 'text': 'Figure 7-50 Attacker Aiming for the Critical V2X Slice', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 532, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '356659807094f1160d5541d835b52697', 'text': 'Step 3. Once the attacker takes control of the MEC application dedicated for critical slices, such as V2X, it could lead to disastrous consequences. In the example shown in Figure 7-50, the attacker gains access to the V2X MEC application using the vulnerabilities in the host software and hardware.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 532, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '45950a82207402f210ae6c862e8b92b8', 'text': 'Step 4. As indicated in Figure 7-50, the attacker could perform a denial of service by rejecting all messages from the V2X application in the vehicles to the MEC application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 533, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0e488ba97f2c9f15521142d9efd8e44e', 'text': 'Figure 7-51 illustrates another threat vector due to inadequate security controls in network slice deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 533, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ab96e676bfe44510fc27a41e537d956b', 'text': "Common 5G NFs for all lices RAN Layer Edge Layer ' “MEC Slice #1- V2X Slice 0 Common PCF UPF Ea i Common f— AMF SMF MEC Sliog #1a - V2X Slie Appin Infernet/ Apps ¢ NRF PCF UPF AVF UPF It § i Slice #2 - MBB Slioe 9 | Appin M 1 MEC 0 ternet NRF UPF Internet/ Apps AMF Appln o= 3 PCF UPF Command & Slice #3-1oT Siice Control Center Internet/ Apps", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 533, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ce1095b8b029345c00bf21976475c030', 'text': 'Internet/ Apps', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 533, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8fc627da44969660323415b0208be1b4', 'text': 'Figure 7-51 Data Exfiltration and Data Hoarding Due to Insufficient Security Controls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 534, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd47f4e7bd8be6ff24d5a52b987d8fa89', 'text': 'Step 5. Once the MEC applications for all the slices are under the attacker’s control, the attacker could send unauthorized commands such as bulk exporting the parameters from the V2X application and exporting the information from the database connected to all the MEC applications to a C2C server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 534, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '40876cfcd86ea1860635ffceb287d7d3', 'text': 'Step 6. The attacker could then analyze the collected data in the C2C server to understand your network and its vulnerabilities better to perform attacks on all the vulnerable software and hardware components in the slice network and applications of the devices being catered for by the slices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 534, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '24bb7b27076b2b7d9d8e8036d7bc8bab', 'text': 'Mitigations: Case Study', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 534, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '10ce49a457c03b0e4a478e378a18d8ed', 'text': 'This section will take you through the mitigation steps to secure the network slice deployments enabled by SDN and orchestration components. This section will be of particular interest to readers trying to understand the exact scope of the threats and what specific solutions could be used as a tactical method to mitigate the threat vectors discussed under the “Threats: Case Study” section earlier in this chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 534, 'parent\_id': '24bb7b27076b2b7d9d8e8036d7bc8bab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aa69750bd2af803f82891d8bd2953c33', 'text': 'Figure 7-52 shows the multilayered security controls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 534, 'parent\_id': '24bb7b27076b2b7d9d8e8036d7bc8bab', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '19a253d5ad2dfdff746e6c2919a96438', 'text': '[AM policy per slice 0 MEC Transport and 5G NFs Slice 1 Ea RAN 4 Slice Level Infernet / Apps Monitoring & Anomaly Detection Slice 2 ll " - Ii gNB (ou +Cu) 550 Internet / Apps =l Slice 3 B -/ i{\\', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 535, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eec353af12d302d181ee8ce57d33ca12', 'text': 'Figure 7-52 Key Security Controls to Secure the Network Slice in the Deployment Example', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 535, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5a34db9748e24be0613c80d2b8be75ad', 'text': 'Figure 7-52 illustrates the five key security controls to mitigate the threats discussed in the “Threats: Case Study” section. The five key security controls are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 536, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4ed6e268919ce05dcf83d3cb34a0f7b1', 'text': '1. Global Policy Engine', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 536, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '161ebb93aba9dcd1cdbb35cc4f1f653f', 'text': '2. IAM policy per slice', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 536, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '20d2b659e36eb3babea2effc82f3e35d', 'text': '3. Application-level policy per slice', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 536, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cac06601fb06c97e3d1c287bc8ed27ed', 'text': '4. API security policies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 536, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f33b7def155a3b5e6159074e91e7a41', 'text': '5. Slice-level monitoring and anomaly detection', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 536, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8938b1eae741e4442b11d0e7acf0a8f2', 'text': 'To clarify the threat mitigation better, security controls are shown in the physical design in Figure 7-53 and described in the list that follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 536, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '46abf6fb14089862b7392f16a9840e20', 'text': 'Network & Application- Custom global policy to restrict and control levetlomety Data Collection & users & devices AP! validation, Anomaly detection Authentication & per slice ‘Internet \\ Authorization\\ [ 0 API GW | WAF ToR switches ToR switches Centralized 56C MEC Backhaul Application-level policy AM per enforcement & slice Vunerabilty management per slice TLS encryption TLS encryptio - [ pm- pom- - i | n { h ”. I h 5 L - - (% i- —————— il =l - Load T2 0 — | UPF \_ NRF - 51 0 — | NFs NFs Appln \_ al = al = T — | al al slices =) slices \_ slices slices T T', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 537, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d4317cdc473790d40ec807ffc4e718c', 'text': 'Figure 7-53 Key Security Controls Mapped to Actual Design of the Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 537, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7952c7821824fb77c12ad2d68d4b66e1', 'text': '1. Global policy: The global policy engine can be considered the brain of the policy distribution and enforcement layers. You can apply custom rules to the global policy engine, which then is responsible for the final decision on granting access to users and devices. The global policy engine is then paired with the Identity and Access Management solution to ensure that the policies are applied to all the users and devices accessing the slice components, including the host on which the slice network functions are', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 537, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0034f52cdd13c1c7e9467793dccdbe6c', 'text': 'deployed. This topic is well covered in the section “Segmentation and Monitoring of the Management Layer.”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 538, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67c784a274c61c75afc188c24223d8fb', 'text': '2. Identity and Access Management (IAM): IAM ensures that repeated authentication and authorization based on zero-trust principles are applied to all the users and devices accessing the host software and hardware. It would generate any session-specific authentication and authentication token or credential used by a client to access an enterprise resource. This layer is also responsible for enabling, monitoring, and eventually terminating connections between users, devices, and the network devices and slice-level NFs. The IAM layer should be able to be integrated with local and external data sources such as industry-compliance systems, threat intelligence feeds, public key infrastructure (PKI), ID management systems such as LDAP servers, and security information and event management (SIEM) solutions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 538, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '117d244750c2fbe8df2fd49c96112f7b', 'text': '3. Application-level policy enforcement: This layer ensures that application- level policy enforcement is applied to individual NFs deployed on the hosts. With the evolution of 5G deployments, the data centers will grow larger and much more complex, with hundreds or thousands of interdependent 3GPP and non-3GPP NFs. This will lead to a continual rise in complexity due to an increase in east-west traffic, application onboarding, virtualization, containerization, security threats, and cloud migrations for 5G-specific network functions. Having application-level security policies would help in enabling application-level access user and device policies instead of users and devices allowed access based on a pool of IP address. The chosen solution should also provide the following functionalities:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 538, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b19ebffb94009ef802209f1036e41e2d', 'text': '• The solution should be able to gain complete visibility into slice- level NF and application components and their dependencies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 538, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fb2577b4976d19fbfc506cea131d66cb', 'text': '• The solution should automatically generate microsegmentation policy based on application behavior.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 538, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ef6793380b0ad71afae7125b7708f70f', 'text': '• The chosen application-level policy enforcement should provide a mechanism to integrate with your global policy engine.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 538, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8da4e13b96b76e89f80e936c790503e6', 'text': '• The solution should enforce the application-level policy across all 5G multicloud workloads consistently. This will help to minimize any lateral movement of the attacker.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 538, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '661c822819456ae7af383e977430480a', 'text': '• The solution should be able to identify software vulnerabilities and exposures to reduce the attack surface.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 538, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '89fc930f45d224d66f67ea288d526182', 'text': '• The solution should provide process behavior baselining and identify deviations for faster detection of any indicators of compromise (IoCs).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 539, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6a629b40dd45325a90642af0a0fb4045', 'text': '4. API gateway: The API gateway or web application firewall (WAF) layer is used to secure the API calls within the network slices. This includes the API calls from the NSaaS slice reseller and slice consumers toward the service providers. The API gateway will enforce access and authorization validation using the custom policies applied by the global policy engine on all API calls within the 5G network slice components using standard authentication, token generation, and multifactor authentication. Some of the key capabilities are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 539, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c0f7e7f19ec22a03ade611a44851071c', 'text': '• The solution should allow custom rules to be deployed or should be able to be integrated with an external global policy engine.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 539, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '14b08388bc8bd25b71a6df4923725fe6', 'text': '• The solution should include multiple security models with ML and AI integrations to provide enhanced mitigation against zero-day attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 539, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd3325b0fbc3c7c43b8d015f21bba4ea0', 'text': '• The solution should be able to terminate TLS sessions, such as HTTPS sessions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 539, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '25ffdfea8f3f4b52bb7a8776c64a4921', 'text': '• The solution should be able to be implemented at any location (on- premises as well as public cloud).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 539, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0520cbc4be51fd0ce4b40fe2d5ce09b3', 'text': '• The solution should provide visibility on the inbound and outbound web traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 539, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a53dbedc6329c120df41dc1ea9d2302b', 'text': '• The solution should provide multiple options to configure the rules (for example, using CLI, UI, and API).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 539, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '13a20cecd8713ef3fdc3d1c7f4ddef26', 'text': 'The key capabilities are further discussed in the “4. Secure API” section within this chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 539, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '45c15cb7ccee5f3a8229f04ffb18238e', 'text': '5. Monitoring and anomaly detection: To ensure end-to-end monitoring and any anomaly in all network slices, a robust monitoring and anomaly detection solution should be deployed. Such solutions should provide end- to-end visibility at the slice level. You should be able to create rules per slice level, such as slice 1 should not interact with slice 2 and so on. Any variations from such rules should create an alert using which further investigations can be carried out. User-based per-slice rules should also be applied and any breaches identified. For example, User 1 usually interacts with Slice 1. An instance gets noticed when User 1 tries accessing the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 539, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9e63d8f799b3fa4ca89af1d947a0905b', 'text': 'management of Slice 2. This is an anomaly in behavior, and an alert is sent to the security team and can then be investigated further.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 540, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5b618ae689acb68462614f2e3c23cf80', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 540, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eed58242630dab6e6525ef25f991966b', 'text': 'As discussed in this chapter, network slicing will enable you to create an independent end-to-end logical network that runs on a shared physical infrastructure, capable of providing a negotiated service quality. The “Threats: Case Study” section took you through the different threats in the network slice deployment using SDN and orchestration, the mitigations of which were explained in the “Mitigations: Case Study” section. The section “Real Scenario Case Study: Threats in the 5G Network Slice, SDN, and Orchestration Deployments and Their Mitigation” took you through the multidomain threat examples and their mitigation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 540, 'parent\_id': '5b618ae689acb68462614f2e3c23cf80', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '82297b6fe0875aa621d51fff608b7377', 'text': 'Figure 7-54 shows you the multilayered security controls to secure the multiple layers for network slice deployments, including SDN, orchestration, and NSaaS layers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 540, 'parent\_id': '5b618ae689acb68462614f2e3c23cf80', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '7e7002d9f67b68f716d4bf891ec60179', 'text': 'NIV W VIHIUIT VI VHTVWU WUV OF T ENT Device / loT Orchestration I ammmmam=e MVNMS / SDN Enterprise loT GW/ Controller Controller Slice 1 pmmmmmm—————— §GC CNF deployed on Cloud dedicated to Slice 1 Slice 1 ilia F— é Slice 2 . — Slice 2 ;m —( (A) NB (DU+CU) E §GC CNF deployed on-premises Slice 3 : \_D\_ dedicated to Slice 2 Ceessscnanana? anspo Slice 3 5GC CNF deployed on-premises dedicated to Slice 3 S I —', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 541, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6e58544088bc5e470f9140a394425568', 'text': 'Figure 7-54 End-to-End Security Controls to Secure Network Slice Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 541, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a830c193d612365575364c1a7073e768', 'text': 'Figure 7-54 shows the key security controls required to secure the various modes of network slice deployment. It has to be noted that you can share the security controls for other parts of the infrastructure if your 5G network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 541, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bc44a85a0da9c00e28503fd5589446e8', 'text': 'deployment has other parts of the 5G infrastructure, such as 5G RAN, 5GC, and 5G MEC. The security control layers are summarized as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 542, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '33c2e530088eafd10f86eb6b072ab142', 'text': '• Built-in hardening (hardware and software layer): Network slice– related use cases are heavily dependent on the SDN and the orchestration layers. The vendors you choose for this layer should have a robust secure lifecycle process for developing the software, creating and applying the software update patches, and so on. SDN and orchestration layers will require automation to perform provisioning and dynamic scaling of the 5G 3GPP and non-3GPP network functions. Built-in hardening and security features of the vendor are important and should provide secure provisioning servers and secure communication with the provisioning servers. The SDN and orchestration solution being used should also encrypt data and separate management and production network traffic for additional isolation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 542, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '344eae9a0a64544cfd27f17bde6e052d', 'text': 'The list provided in the “Hardening Hardware and Software” section in Chapter 5, “Securing MEC Deployments in 5G,” is a good place to start the checks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 542, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3bab41f7b5323c9b27ff16da3c56828d', 'text': '• Enhanced access control layer: Access to the network slice layers, such as the service layer, orchestration, SDN, and 5G network functions should be granular, role based, and should be applied at the slice level. Once your 5G network is mature, you will start deploying network slice as a service (NSaaS) business models. To provide mitigation of risk vectors such as unauthorized access in NSaaS deployments, it is recommended to have robust and granular access controls. Access for all the slice users should be restricted, and access should be provided only for their specific slice components. Any deviation of the user’s behavior should have an alerting process involved to indicate the change in behavior.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 542, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '895207c43c5739f69e61e03dca4ba248', 'text': '• Application protection and policy enforcement: The solution used for application protection and policy enforcement should scan all images before they run and should enforce policy checking to ensure they are allowed to be executed in your environment. Such scans should also prevent the deployment of untrusted and vulnerable images and have the capability to block containers violating the runtime model based on the configured runtime rules. The policy enforcement layer should ensure you can optimize your multivendor firewall policy by updating it based on the application behavior, and it should remove access for third-party MEC applications that are decommissioned. The application protection and', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 542, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dc9285e910862b054d0916bafe156bad', 'text': 'policy enforcement layer should also provide vulnerability assessment and any forensics capabilities to investigate any abnormal user or application behavior.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 543, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '13cb0f17373be4c995058ae50dfcc4d2', 'text': '• Enhanced visibility, anomaly detection, analytics, and monitoring: The key to mitigating sophisticated malware attacks is to detect any anomaly within the MEC by using behavioral analysis, which could potentially detect the malware scanning, connection, and propagation throughout the network. Another type of attack that could be detected by enhanced visibility and monitoring is an attack taking place using the encrypted traffic, such as data being exfiltrated to a C2C server. The analytics part of this solution must also use the threat intelligence feed and combine this with the analysis of the gathered information using ML and AI algorithms to proactively detect any change in network behavior.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 543, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ac3b3d3f2fa219d8f589833ec2ca3a41', 'text': '• API security: Orchestration and SDN layers use API for northbound interface (NBI) communications. The service layer uses an API to interact with the external NSaaS consumers and non-NSaaS consumers. Securing these API communications is very important because attackers will try to exploit the vulnerabilities within the API implementation and the web server to attack the critical network slices. You should carry out audits for your API communication, both in the trusted and nontrusted environments. Having a strong, secure API strategy, such as conducting penetration tests and audits on the APIs and applications using APIs, will ensure that your API is secure and any security holes/gaps are understood. The gaps can then be filled by ensuring the right feature or capability is enabled within the relevant security control, such as integration with the global policy engine to ensure granular access control for each API request from the NSaaS consumers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 543, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a6369b47457bc71ac80d6444ca2f8298', 'text': '• NGFW, advanced anti-malware, and anti-DDoS: The implementation of network slices should consider multiple layers of security controls due to the high interaction with untrusted zones and would require encryption of the data being transferred between the enterprise sites and your 5G network slice components, such as the Network Exposure Function (NEF), which should be protected by application-aware firewalls. Segmentation of traffic should be provided by an application-aware next- generation firewall (NGFW) that can filter traffic based on the application rather than just port and IP address. The NGFW should be able to utilize global threat intelligence feeds, consume telemetry data from applications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 543, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0d8da0e76e62a8660b22a009f168fd4b', 'text': 'and the network, and co-relate files and create context-aware knowledge to detect malware and identify patterns to indicate possibilities of zero-day attacks. DDoS protection should include rate limiting and should have a robust ML and AI engine to detect and mitigate attacks faster.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 544, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '72e3abc1ced9658eafd36cdaad449d03', 'text': 'Key Acronyms', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 544, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '59cc77b3672811ba75906628a8101f35', 'text': 'The following table expands the key acronyms used in this chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 544, 'parent\_id': '72e3abc1ced9658eafd36cdaad449d03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'd21fb660a54da86a02bac72a24106e01', 'text': 'Acronym Expansion 5GC 5G Core AMF Access and Mobility Management Function API Application programming interface c2C Command and control CA Certificate authority CAPIF Common API Framework CD Continuous Development CI Continuous Integration CNF Cloud-Native Function CoPP Control Plane Policing CP Control plane CU Centralized Unit CUPS Control Plane User Plane Separation DCT Docker Content Trust DDoS Distributed denial of service DPP Data Plane Policing DU Distributed Unit EAP Extensible Authentication Protocol ESP Encapsulation Security Payload', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Acronym</th><th>Expansion</th></tr></thead><tbody><tr><td>5GC</td><td>5G Core</td></tr><tr><td>AMF</td><td>Access and Mobility Management Function</td></tr><tr><td>API</td><td>Application programming interface</td></tr><tr><td>c2C</td><td>Command and control</td></tr><tr><td>CA</td><td>Certificate authority</td></tr><tr><td>CAPIF</td><td>Common API Framework</td></tr><tr><td>CD</td><td>Continuous Development</td></tr><tr><td>CI</td><td>Continuous Integration</td></tr><tr><td>CNF</td><td>Cloud-Native Function</td></tr><tr><td>CoPP</td><td>Control Plane Policing</td></tr><tr><td>CP</td><td>Control plane</td></tr><tr><td>CU</td><td>Centralized Unit</td></tr><tr><td>CUPS</td><td>Control Plane User Plane Separation</td></tr><tr><td>DCT</td><td>Docker Content Trust</td></tr><tr><td>DDoS</td><td>Distributed denial of service</td></tr><tr><td>DPP</td><td>Data Plane Policing</td></tr><tr><td>DU</td><td>Distributed Unit</td></tr><tr><td>EAP</td><td>Extensible Authentication Protocol</td></tr><tr><td>ESP</td><td>Encapsulation Security Payload</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 545, 'parent\_id': '72e3abc1ced9658eafd36cdaad449d03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '678e405c17293f0e4be11ee749691e02', 'text': 'FH Front haul FIPS Federal Information Processing Standard HSM Hardware security module HTTPS Hypertext Transfer Protocol Secure IAM Identity and Access Management IPsec [P security ISAKMP Internet Security Association and Key Management Protocol M2M Machine-to-machine MAC Medium Access Control MEC Multi-access edge compute MitM Man in the middle mMTC Massive machine-type communication NEF Network Exposure Function NR New Radio NRF Network Resource Function NSA Non-standalone NSaaS Network slice as a service NSSF Network Slice Selection Function RBAC Role-based access control SDN Software-defined network SLA Service level agreement TLS Transport Layer Security', 'metadata': {'text\_as\_html': '<table><thead><tr><th>FH</th><th>Front haul</th></tr></thead><tbody><tr><td>FIPS</td><td>Federal Information Processing Standard</td></tr><tr><td>HSM</td><td>Hardware security module</td></tr><tr><td>HTTPS</td><td>Hypertext Transfer Protocol Secure</td></tr><tr><td>IAM</td><td>[dentity and Access Management</td></tr><tr><td>IPsec</td><td>[P security</td></tr><tr><td>ISAKMP</td><td>Internet Security Association and Key Management Protocol</td></tr><tr><td>M2M</td><td>Machine-to-machine</td></tr><tr><td>MAC</td><td>Medium Access Control</td></tr><tr><td>MEC</td><td>Multi-access edge compute</td></tr><tr><td>MitM</td><td>Man in the middle</td></tr><tr><td>mMTC</td><td>Massive machine-type communication</td></tr><tr><td>NEF</td><td>Network Exposure Function</td></tr><tr><td>NR</td><td>New Radio</td></tr><tr><td>NRF</td><td>Network Resource Function</td></tr><tr><td>NSA</td><td>Non-standalone</td></tr><tr><td>NSaaS</td><td>Network slice as a service</td></tr><tr><td>NSSF</td><td>Network Slice Selection Function</td></tr><tr><td>RBAC</td><td>Role-based access control</td></tr><tr><td>SDN</td><td>Software-defined network</td></tr><tr><td>SLA</td><td>Service level agreement</td></tr><tr><td>TLS</td><td>Transport Layer Security</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 546, 'parent\_id': '72e3abc1ced9658eafd36cdaad449d03', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '38dc24a55b1f68de3bf6a366309fcafa', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 547, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '62ae97b57b31154bdcb1d894b003e9ea', 'text': '3GPP TS 28.530 V17.0.0', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 547, 'parent\_id': '38dc24a55b1f68de3bf6a366309fcafa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd6a0964f4c63570fdeac45f83fbc6ce7', 'text': '3GPP TR 33.813 V16.0.0', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 547, 'parent\_id': '38dc24a55b1f68de3bf6a366309fcafa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5339d91f0af36b8ec8c36cb168b90607', 'text': '3GPP TS 24.502 V17.1.0', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 547, 'parent\_id': '38dc24a55b1f68de3bf6a366309fcafa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c86621135c8e6f902ee97c2cd472594e', 'text': '3GPP TS 23.501 V16.9', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 547, 'parent\_id': '38dc24a55b1f68de3bf6a366309fcafa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9164b3f9743130403a646f4f726a1fc4', 'text': '3GPP TS 23.502 V16.7.1', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 547, 'parent\_id': '38dc24a55b1f68de3bf6a366309fcafa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c35456f02f53c78486b7ad5dbfb508e3', 'text': 'NIST SP 800-207', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 547, 'parent\_id': '38dc24a55b1f68de3bf6a366309fcafa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '65c9943231c4b2993301fd581cc8cf82', 'text': 'OWASP.org', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 547, 'parent\_id': '38dc24a55b1f68de3bf6a366309fcafa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f52a9c0f3b208163e421a2ca4318e407', 'text': 'https://www.cisco.com/c/en\_uk/solutions/data-center-', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 547, 'parent\_id': '38dc24a55b1f68de3bf6a366309fcafa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7f6da028eab9b23ae4b5eafb19e7fcb1', 'text': 'virtualization/application-centric-infrastructure/', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 547, 'parent\_id': '38dc24a55b1f68de3bf6a366309fcafa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '40d1ea9c483137fcb9d0863195569981', 'text': 'systems-management/network-services-orchestrator/nso-bridge- automation.pdf', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 547, 'parent\_id': '38dc24a55b1f68de3bf6a366309fcafa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5e403e460387558039a8211d6c210705', 'text': 'https://www.openpolicyagent.org', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 547, 'parent\_id': '38dc24a55b1f68de3bf6a366309fcafa', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '85b20146f4de984ff57dd7c022741d18', 'text': 'Chapter 8. Securing Massive IoT Deployments in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '89c2695dde7d62f1076c81250705affa', 'text': 'After reading this chapter, you should have a better understanding of the following topics:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a7a00f0d27d88a9f3debe8c385f1a4a', 'text': '• Threats in massive IoT use case deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6d0a741803794386f7aeb255f0ac1e38', 'text': '• Securing massive IoT networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b3c244e4181194dda5bb4195f8a3a74b', 'text': '• Real scenario case study examples of Massive IoT threat surfaces and threats mitigation techniques', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '906754b66e226d1bf7edb919baf4003c', 'text': 'This chapter will take you through the threat surfaces in 5G massive IoT deployments and mechanisms to mitigate the threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'afd9513168f97ae86b3a906698a55c37', 'text': 'This chapter will be of particular interest to the following teams from enterprise, industry verticals, Non-Public Networks (NPN), 5G service providers deploying 5G mIoT and cybersecurity vendors planning product developments and new functionalities to secure 5G mIoT use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4dda3d4c39e1c6f0e5db925882ce53b4', 'text': '• Mobile infrastructure strategy teams of service provider deploying mIoT in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '70386ddd0151263b313237a395312c51', 'text': '• Security strategy teams within service provider and enterprise verticals planning on deploying 5G mIoT', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '15d0539686b60864f619db045a515146', 'text': '• Transmission and the packet core team within service providers and private 5G enterprises planning to deploy 5G mIoT', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '332d397aa9f3328b1bdc69b4a3a2e75b', 'text': '• Cloud computing and data center teams involved with 5G strategy and deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5d195a027f38ae7d529f59d3eb7b6dac', 'text': '• Security architects and design teams looking at securing the public and non-public mobile infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7f144c1b223a826e7fab3063a02bd575', 'text': '• Solution and security architects deploying 5G mIoT on enterprises and industry verticals', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '85bc9f446129a64046e5ae3f8662a044', 'text': '• Enterprise solution and security architects using IoT services from mIoT service provider', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 548, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '51d29df8b2e35faf9b7242667f771ba9', 'text': '• Government departments deploying 5G mIoT', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 549, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1b5be5e7a67c799aca65f79af2c04862', 'text': '• Cybersecurity vendor teams looking to secure mIoT deployments for their customers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 549, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b85b59b58f3a827e48c564d8b4001308', 'text': '• Product managers of cybersecurity vendors trying to identify use cases for new products or features to protect 5G mIoT deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 549, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd8b6002bc0eaa9050e319b32a75dfc48', 'text': '5G represents a disruptive shift from just traditional consumer smartphones to advanced enterprise services, including ultra-reliable low-latency communication (URLLC) –based machine-to-machine (M2M) use cases. 5G is expected to be widely adopted in enterprise, industrial, and IoT use cases, enabling greater workforce mobility, automation, and countless new applications. Incorporation of 5G into these environments requires a deeper level of integration between end-user networks and 5G service interfaces, exposing both enterprise owners (in particular, operators of critical information infrastructure) and 5G service providers to new risks. Before we get into the risks and mitigation of risks, we will first need to look into the types of IoT use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 549, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'de7c849a4393909328b7711b2382260b', 'text': '5G also sees a departure from the reliance on a single approach to authenticating all users onto the network-based on SIM cards. The Third- Generation Partnership Project (3GPP) has addressed such shortcomings, with 5G now integrating the Extensible Authentication Protocol (EAP) framework, first adopted by Wi-Fi into WPA-Enterprise back in 2002, into its architecture. The 5G standard now provides examples of how to use EAP-TLS certificate- based authentication in 5G as well as other EAP methods that support mutual authentication. The list that follows outlines some of the key reasons why IoT threats are quite critical in 5G based on the excerpts taken from the Cisco Annual Internet Report (2018-2023):', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 549, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '420001f76b0f99d5d7e112ac2cb524e1', 'text': '• The number of devices connected to IP networks will be more than three times the global population by 2023. There will be 3.6 networked devices per capita by 2023, up from 2.4 networked devices per capita in 2018. There will be 29.3 billion networked devices by 2023, up from 18.4 billion in 2018.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 549, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b3ba3779daccd7bc1d4067b0c5cb5505', 'text': '• Globally, devices and connections are growing faster (10 percent compound annual growth rate [CAGR]) than both the population (1.0 percent CAGR) and the Internet users (6 percent CAGR). This trend is accelerating the increase in the average number of devices and connections per household and per capita. Each year, various new devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 549, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d7cb964ca641cab5fbadfd2b15b7b93', 'text': 'in different form factors with increased capabilities and intelligence are introduced and adopted in the market. A growing number of M2M applications, such as smart meters, video surveillance, healthcare monitoring, transportation, and package or asset tracking, are significant contributors to the growth of devices and connections. By 2023, M2M connections will constitute 50 percent of the total devices and connections.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 550, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dd1fdcd4b81365b663348d584f9b2442', 'text': '• M2M connections will be the fastest-growing device and connections category, growing nearly 2.4-fold during the forecast period (19 percent CAGR) to 14.7 billion connections by 2023.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 550, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0d4a16f4ca389f7dfcec44844ab3c48a', 'text': 'With this type of growth in the number of devices and spurts in new use cases such as M2M, an attack that successfully disrupts the network, or that steals or undermines the integrity of confidential data, could have a far greater economic and societal impact than previous generations.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 550, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '13a855b4cfa76eb15d7fc4d9796c41be', 'text': 'IoT devices and applications have been around for quite some time and are not a new concept for 5G. There are networks today using LTE or NB-IoT technologies enabling IoT use cases. 5G offers flexibility in IoT deployment. The use cases aimed at 5G IoT are devices having different bandwidth requirements. Some require high bandwidth and transmit in burst, while some require low bandwidth and continuous connectivity. 5G offers this capability to support the massive number of devices with different bandwidth requirements. In addition, 5G also supports enterprise and industry use cases that have strict requirements on latency. This is one of the key reasons why the industry is looking at adopting 5G. The flexible mode of 5G deployment using network slicing and deployment of applications in the edge of the network can bring down the latency to 1ms or less, enabling ultra-reliable and low-latency use cases such as factory automation, enhanced vehicular technologies such as vehicle-to-everything (V2X), power and utility sector use cases such as smart energy grids, and other demanding use cases to become a reality.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 550, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f7fb585c76c698192b3d9728eacd8323', 'text': 'There are different types of IoT use cases in 5G depending on the data consumption, energy consumption, and scale of deployment. When you take a step back and look at the use-case scenarios in 5G, we can split the IoT devices into smart devices and not-so-smart devices. Smart IoT devices are the devices that have some intelligence built into them and can make some decisions based on the input data. The not-so-smart IoT devices are the devices that just send the collected data and receive certain actions, such as stop data collection and a query to start data collection.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 550, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8f6f46ab5ffdc0e22790052112c23157', 'text': 'Use cases attributed to 5G such as smart cities would require the use of both types of devices, as shown in Figure 8-1, and have an artificial intelligence (AI), machine learning (ML), and an analytics layer to analyze the information from multiple devices and make a decision based on it. An example could be automated car parking in a busy area such as an airport parking lot, as shown in Figure 8-1.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 551, 'parent\_id': '85b20146f4de984ff57dd7c022741d18', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ac17cbf33da646e79058d9a3500d80e7', 'text': 'Analyncs T MEC Public cloud & Internet i VW@ Movable Autonomous Cargo Parking spot Emergency Sensor sensor Unit Vehicular CCTV sensor Pedestrian system system', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 551, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e61b3190ef7ae576737b7e6078aaa59e', 'text': 'Figure 8-1 Different IoT Device Types to Enable a 5G Smart City', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 551, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd8bca5a8a08246b8741af080d31631ae', 'text': 'As shown in the Figure 8-1, it would require different types of mIoT devices to enable the smart city use case. Table 8-1 lists the types of devices to fulfill the use case of finding a parking spot and the safest way to reach the parking spot.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 551, 'parent\_id': 'e61b3190ef7ae576737b7e6078aaa59e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'e7af8f2d89469b7200c0b361fb76b8b5', 'text': 'IoT Device Cargo sensor Not-so-smart device Sends the geo-location metadata along with the speed Parking spot Not-so-smart device Indicates whether or not a vehicle is sensor located in a parking spot Emergency Unit Not-so-smart device Indicates whether an emergency Vehicular system vehicle is active in the location Movable CCTV Not-so-smart device Detects if there is movement near the sensor parking spot Autonomous Smart device Indicates any V2X application in the pedestrian system vicinity and broadcasts a message based on whether or not a pedestrian is crossing. Captures any speeding instances and sends data to the road safety officers. Indicates any collision and immediately broadcasts messages to the emergency health unit. V2X Smart device Provides a road safety application such as intersection movement assist, provides emergency brakes, and also includes V2V (vehicle-to-vehicle) communications', 'metadata': {'text\_as\_html': '<table><thead><tr><th>IoT Device</th><th></th><th>oDk [P</th></tr></thead><tbody><tr><td>Cargo sensor</td><td></td><td></td></tr><tr><td>Parking spot sensor</td><td></td><td></td></tr><tr><td>Emergency Unit Vehicular system</td><td></td><td></td></tr><tr><td>Movable CCTV sensor</td><td></td><td></td></tr><tr><td>Autonomous pedestrian system</td><td>Smart device</td><td>Indicates any V2X application in the vicinity and broadcasts a message based on whether or not a pedestrian is crossing. Captures any speeding instances and sends data to the road safety officers. Indicates any collision and immediately broadcasts messages to the emergency health unit.</td></tr><tr><td>V2X</td><td>Smart device</td><td>Provides a road safety application such as intersection movement assist, provides emergency brakes, and also includes V2V (vehicle-to-vehicle) communications</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 552, 'parent\_id': 'e61b3190ef7ae576737b7e6078aaa59e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aabe462371c5cddf2ee13732f28ac96e', 'text': 'Table 8-1 Different IoT Device Types', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 552, 'parent\_id': 'e61b3190ef7ae576737b7e6078aaa59e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '32372806400045a4908610015cad2c2e', 'text': 'As listed in the Table 8-1, to fulfill this example of smart city–based parking, there is a need for both not-so-smart-devices and smart devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 552, 'parent\_id': 'e61b3190ef7ae576737b7e6078aaa59e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9142ee20071b8671336104f1c9d91d2b', 'text': 'In this example, the cargo sensor, Emergency Unit Vehicular system, and autonomous pedestrian system are all part of the collision-prevention mechanism. The parking spot sensor and movable CCTV sensor are part of the parking detection mechanism. The V2X system is embedded within the vehicle for passing along the metadata to the MEC application.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 552, 'parent\_id': 'e61b3190ef7ae576737b7e6078aaa59e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '76a4e19a8f9010e565eae02153e8a1f4', 'text': 'All the data from the mIoT devices is then passed on to the AI and ML system and real-time (RT) analysis system. The AI, ML, and analytics system will then detect the free parking spot and the safest way to approach the parking spot and then help park the car or indicate the parking spot and the best way to reach it.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 553, 'parent\_id': 'e61b3190ef7ae576737b7e6078aaa59e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f329f3392c894c1a3777f6506c84f566', 'text': 'Massive IoT in 5G addresses the need to support billions of connections with a range of different services. IoT services range from device sensors requiring relatively low bandwidth to connected cars that require a similar service to a mobile handset. Network slicing provides a way for service providers to enable services to enterprises, giving them the flexibility to manage their own devices and services on the 5G network. mIoT, as the name suggests, is a category of use cases that is driven by scale.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 553, 'parent\_id': 'e61b3190ef7ae576737b7e6078aaa59e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0c76692b97492a920d494e73c1fb394b', 'text': 'Figure 8-2 illustrates an example of components that are part of the mIoT deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 553, 'parent\_id': 'e61b3190ef7ae576737b7e6078aaa59e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '555466ed2530f9bd2e0dbe6b06fed7a4', 'text': '\*‘ Sensors W SP1oT Applications & W Internet Vehicular Asset tracking [Rpep—— = e — | gNB MEC Centralized DC UEs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 553, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '93401f94928f02ad15f515fc926963a3', 'text': 'Figure 8-2 mIoT Deployment in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 553, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5b1413dca1935a555cf5725631274cd0', 'text': 'Figure 8-2 shows an example of mIoT use-case deployment using 5G. The gNB serves geographically disparate devices such as sensors and vehicles that', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 553, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'af574cad9885224a9515a5ce5f9b7b31', 'text': 'need to be tracked. mIoT would typically include devices that transmit and consume low data and are in the scale from hundreds to millions. Depending on the device type, it could be low-energy-consuming devices with limited access to power with a very light software stack for communications. There are device vendors in the market with 5G-capable chips with optimized power consumption.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 554, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3ef0c98c944440f3a55cd234a7ecd1bd', 'text': 'This chapter will cover the 5G MIoT part. 5G IoT use cases based on smart devices (V2X, smart city, industrial IoT use cases, and so on) are covered in Chapter 9, “Securing 5G Use Cases”).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 554, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '51d318d82d39337e8de879056e0bb344', 'text': 'Massive IoT–Based Threats in 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 554, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e4fc1004bea342084a1ab26defe22bdc', 'text': 'Figure 8-3 shows the key threats for the device-based threats for the devices connecting to the service provider’s 5G infrastructure. The devices in this case can be the 5G user equipment (UE), sensors, and IoT devices connecting to the 5G network provided by the service provider.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 554, 'parent\_id': '51d318d82d39337e8de879056e0bb344', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '9ccef4e38567daa4b722b01a5f2d64b1', 'text': "+ Multiple new connection request + Bot based attack (artficial) causing control plane causing simulianeous resources o exhaust or cause + Forced resource buffer overflows responselfequest causing DoS overloading on the 5G Core CP + Forced crash/Shutdown dug to messages toffrom oT components leading to Denial of Network malwarg injection casing DoS + Mit attacks in air Service tolegitimate devices + Interfaces from the Application inferface due to weak server to loT Core components encryption are based on the Restful API + DDoS attacks from which can be compromised |oT Network leadingto DoS atlacks on 5G Core components Vo ’((A)) 1 2 MEC / Centralized DC SPloT Applications & Internet buffer overflows \* RFID/Bluetooth snifing and + Malicious code injected nto the 10T applications during update causing eavesdropping on the loT device utdown due to causing messages to be intercepted, devices to cause DDoS attacks on'! 1causing DoS modified and retransmitted with false + Data exfilration caused due to expl information within loT applications tjection on driver ses HW causing - Spoofing another device on the + |oT device provisioning server (CMI network and collect data (siently) explois, leaving the entire loT devic ntanal an InT Malininiie rnda iniantinn laading tn aenavatem anen fn he exnlnited an", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 555, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '24e427abe72005c3e111888fabf3032b', 'text': 'Figure 8-3 mIoT Threat Surface in 5G Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 555, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '263bf7125bb4086a61f61d204bd51e28', 'text': 'Figure 8-3 shows 5G multi-access edge compute (MEC), centralized 5GC (5G Core), public or private cloud-based SP applications, and the Internet access layer. Depending on the deployment plans of the service provider, the 5G User Plane Function (UPF) would be deployed in the MEC, along with any of the IoT applications that require caching. When the UPF network functions are deployed in the MEC, the N6 interface—the interface between the data network (DN) and the UPF—is also configured to allow UE and 5G devices to interconnect with the data network. Depending on the deployment scenario, the 5GC could host the 5G network functions that have low impact with higher latency, such as control plane functions, user plane functions for some IoT use', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 555, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '06257e8335aa74c394b74072d1927ef8', 'text': 'cases, and the operations, administration, and maintenance (OAM) functions. Many service providers are also planning to have the configuration management (CM), fault management (FM), and performance management (PM) for the consumer IoT devices being catered to from the public/private cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '92875bef1debafc800074ce42b0b3203', 'text': 'The majority of the threat surfaces illustrated in Figure 8-3 are primarily due to the device vulnerabilities and the devices being compromised by the command and control (C&C) server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c3f092cf056d25c327a06e0e99662ce4', 'text': 'Here are some of the key threats related to mIoT use cases within the 5G networks:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b1e20ee8465e658d1dc3f9d67e9b9c7c', 'text': '• C&C-based attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e0e9c592681a717bdcb0134bc75b6775', 'text': '• Malicious code injection on the driver that compromises the hardware, causing a denial of service (DoS)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a00601db414ff7eb4fbefecc4d68c8cc', 'text': '• Forced resource buffer overflows causing DoS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '07bfc6707addf3e2d723138607f27b17', 'text': '• Forced crash/shutdown due to malware injection, causing DoS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '93c90d46b7181fd4a760dbe6c56692ed', 'text': '• Compromised protocol on an IoT device, causing malicious code injection on the primary device connected to the IoT device', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6383f5cfb2c54a7a9d9032fad81401e8', 'text': '• Firmware OS hacking/code injection, leading to a compromised device', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '86aae8fae8520bff05def37c2e4ee098', 'text': '• Radio-frequency identification (RFID)/Bluetooth sniffing and eavesdropping on the IoT device, causing messages to be intercepted, modified, and retransmitted with false information', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4d668ecaa20b125a0abe15d69e88de51', 'text': '• Spoofing another device on the network and exfiltrating data', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a68fc2e55c141633da2362dc33e79564', 'text': '• Malicious code injection leading to the same device being seen at multiple locations with separate IP addresses', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'debbe178ed68c506e02c35a8bbf7029d', 'text': '• Multiplying the number of nodes (artificially), causing increased signaling in both UL/DL', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '24e427abe72005c3e111888fabf3032b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5b38c0aa9256c4650849cfd088b4ea19', 'text': 'Device Vulnerabilities Due to Weak Built-in Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b74cb95f36b0fa0b1d863ce9c4f7053', 'text': 'mIoT devices usually have very weak built-in security mechanisms due to lower price points of the devices to make them affordable to a large consumer base. The IoT deployment of any type, be it based on smart IoT devices or not- so-smart IoT devices needs, to be catered to by robust security controls to', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 556, 'parent\_id': '5b38c0aa9256c4650849cfd088b4ea19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b00f34c5760942ea20bdc4f586aeae99', 'text': 'mitigate the vulnerabilities introduced by weak built-in security is mainly due to the low cost and limitations due to the form factor. Non-mIoT use cases that are not geographically located would also need multilayered security controls to secure them from targeted attacks very specific to industry verticals, such as major automotive manufacturers or government utility verticals.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 557, 'parent\_id': '5b38c0aa9256c4650849cfd088b4ea19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '85df7e828b88f50ec0ffe584330d902c', 'text': 'Spoofing, cloning, and eavesdropping on the 5G endpoints/IoT devices can be carried out by attackers impersonating an RFID or Bluetooth device and reading and recording the transmitted data from the 5G-enabled IoT device. This is primarily made possible due to weak access controls and poor authentication methods used by the IoT device. These kinds of attacks are more prevalent in verticals of IoT such as healthcare where the IoT devices use Bluetooth to transfer the patient’s health statistics to a tablet where the vital stats of the patient can be checked/monitored by the healthcare workers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 557, 'parent\_id': '5b38c0aa9256c4650849cfd088b4ea19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '965ee1bc775a0a70771758c12a4e9732', 'text': 'Another type of attack mentioned in Figure 8-3 is where the devices are compromised. In this instance, all the data from the impacted devices is dropped or redirected instead of being transmitting to the intended receiver for further forwarding or analysis. The data from such devices can then be analyzed by the attacker for any valuable data points, such as the IP address of the receiver, which can then be targeted for DoS.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 557, 'parent\_id': '5b38c0aa9256c4650849cfd088b4ea19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e3926829f6539249de15547602ef3ad7', 'text': 'These kinds of attack methods can also be referred to as sinkhole attacks or a form of routing attack. This is because the method of attack used in such instances is to route the packets away from the main intended receiver. To prevent the detection of such attacks, the data can be mirrored to the malicious data collection server using a method very similar to port mirroring or Switch Port Analyzer (SPAN), which is used quite commonly in the network monitoring environment of the service provider networks. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a dedicated destination switch port for analysis. You can analyze network traffic passing through switch ports or VLANs by using SPAN or Remote SPAN (RSPAN) to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring solution.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 557, 'parent\_id': '5b38c0aa9256c4650849cfd088b4ea19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f3bd5d638f0761ad94629d15e5c299b2', 'text': 'Management layer–based attacks are another key concern for device-based attacks within the 5G. In these attacks, the attacker tries to take control of the key management layers, such as CM, FM, and PM, by exploiting the existing vulnerabilities of the IoT vendors’ management platform or the open source components used in the vendors’ IoT platform. Once the vulnerability has been', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 557, 'parent\_id': '5b38c0aa9256c4650849cfd088b4ea19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5c802c1b9899447c76502f92c996bc82', 'text': 'successfully exploited, the attacker gains access and control over all endpoints catered for by the IoT vendor for the service provider. This can now be used for DoS and distributed denial-of-service (DDoS) attacks. One of the methods the attacker could also use here is to change the encryption type or level (from encrypted to null encryption), which makes the entire IoT network susceptible to man-in-the-middle (MitM) attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 558, 'parent\_id': '5b38c0aa9256c4650849cfd088b4ea19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2813d5020db982e013169b4a3d26668c', 'text': 'The key threat surfaces and vulnerabilities are discussed in more detail in the sections that follow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 558, 'parent\_id': '5b38c0aa9256c4650849cfd088b4ea19', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c720597ddd2190d080c0921abf0526ca', 'text': 'Supply Chain Vulnerability', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 558, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '219b2985eb7e2e0f705f35c177889ef3', 'text': 'Supply chain vulnerability is a well-known issue across different industry segments. The challenge of supply chain vulnerabilities becomes more prominent in 5G, as it enables attaching millions of low-cost IoT devices to the network. 5G also introduces critical infrastructure–based use cases and caters for use cases like smart cities, defense, and so on. These critical infrastructure 5G IoT use cases attract more nation-state attackers and thus are under higher levels of risk for cyberattacks. Supply chain is one of the weak links in security. If not secured properly, it opens the door wide for attacks, and the impacts of the attacks could be devastating, depending on the use case where the vulnerable IoT device was used. This section will take you through the vulnerabilities in the IoT supply chain related to manufacturing and distribution, as shown in Figure 8-4.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 558, 'parent\_id': 'c720597ddd2190d080c0921abf0526ca', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '06a4e74dfdd46c142c0b6f927f7b6111', 'text': 'Requirements il ol o @ oo TEG oL R ) Production ! Logistics d (9 I Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 559, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7c3e2ac45f89e55df0580c28a5415b77', 'text': 'Figure 8-4 Vulnerabilities in Different Stages of the Supply Chain', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 559, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '23bc3de393c5be9c92c81376a4b5ac79', 'text': 'Key vulnerabilities and threat vectors for the IoT supply chain related to manufacturing and distribution are explained in the list that follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 559, 'parent\_id': '7c3e2ac45f89e55df0580c28a5415b77', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5c5885ac6cb7f7a9b54be9e7d30c25f5', 'text': '1. The requirement stage is when you send the requirements for your IoT device to the vendor. This will include details like maximum energy consumption, dimension of the unit, maximum/minimum temperature, pressure (depending on use case), software or platform requirements such as integration options using API, and so on. The threat vector here is the requirement that is actually passed on to the vendor product R&D and manufacturing team. An attacker might add a couple of details in the requirements not actually requested by you. These newly added details are aimed at creating the backdoor using hardware or software remodifications to the original design, which can then be exploited by the attacking entity once deployed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 560, 'parent\_id': '7c3e2ac45f89e55df0580c28a5415b77', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fbc88f7be68915b974ba41bbfb52d397', 'text': '2. The hardware specification team would normally take the requirements from the customer and map them to the required hardware, including deciding what sort of components should be used in manufacturing the device. Typical considerations are values to withstand humidity, temperature, power consumption, and so on. The threat vector here is that an attacker could choose certain components that will fail when a certain condition is met. For example, the malicious actor or the attacking entity could intentionally choose a substandard electronic component or a customized component that fails after a certain temperature or humidity level is reached.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 560, 'parent\_id': '7c3e2ac45f89e55df0580c28a5415b77', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '28a86d6cfa9463b68e283f2e4e02dc3e', 'text': '3. Once the components are finalized, the design team would make a schematic of the design that will be used as a blueprint for the printed circuit board (PCB) manufacturing for the IoT device. This is a very important part of the manufacturing process, as all the further checks on quality and so on would be referred back to the schematic. The attacking entity or the malicious actor could alter the design to include an eavesdropping component to leak sensitive data to a predetermined destination such as a C&C server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 560, 'parent\_id': '7c3e2ac45f89e55df0580c28a5415b77', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '19a52847f9cce2b65a7a60c809773fbb', 'text': '4. The PCB layout process and component soldering are the next steps after the circuit design process. Here, the key vulnerabilities and threat vectors are due to the attacker choosing counterfeit electronic components causing intermittent failures that are difficult to find and correct.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 560, 'parent\_id': '7c3e2ac45f89e55df0580c28a5415b77', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2bbf2e3bdd76747ce485d3a99731bc6d', 'text': '5. IoT software specifications are taken from the requirements list you have provided to the IoT vendor/manufacturer. A member of the IoT software specification team or an attacker working in the software specification team could be directed to modify the specification for the software. The software specification will also be used in the software quality process for validating the software and to ensure that the designed software meets the software', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 560, 'parent\_id': '7c3e2ac45f89e55df0580c28a5415b77', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '569144927b45d0bed295c5248db793ef', 'text': 'specifications. Any modification done in the software specification process will be considered as the software blueprint for the device.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 561, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'adeac1c4efd42e8d052ca988289defda', 'text': '6. The software design team would follow the specifications set by the software specifications team and specify the architecture and software technology to be used. In this process, the vulnerabilities are mainly due to the lack of knowledge about security leading to weak software for the device.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 561, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1ace39865a1e1c30b0833ac59625e1b1', 'text': '7. The software development team programs the IoT device with the chosen software language. With attacks aimed at software vulnerabilities on the rise, it is imperative that the software team follows secure software design and avoids known vulnerabilities such as buffer overflows, which occur when there is more data in the buffer that it can handle, leading to software crash and thus creating a point for cyberattack. This can be intentionally implemented by an attacker within the software development team. Another threat vector is when a team member of the software development team is instructed by an attacker or an attacking entity to include malicious code within the program to allow a backdoor entry to the device or to the private network where the IoT device is deployed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 561, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '20544806c335c0d6b8eb75cfdc91a146', 'text': '8. In the post-PCB layout and software development process, the IoT device manufacturer would validate whether the hardware prototype and software fulfill the requirements set by your (or your customer’s) IoT device requirement. This is the last part of the process when a vulnerability can be identified and patched. If the quality team is compromised by an attacker, the specific vulnerability that is planned to be exploited by the attacker/attacking entity will be overlooked and will not be patched. This will leave the IoT device open for any attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 561, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1ad342e226bb0800fc33a464621c4ebe', 'text': '9. One of the key vulnerabilities in production is shadow production. Shadow production is where the real production numbers are hidden and used to flood the market with IoT devices with backdoors and vulnerabilities, making the devices open to attacks. Another threat vector is where the Joint Test Access Group (JTAG) ports are left unsecured. JTAG is an interface that provides an option for debugging, reprogramming, and so on. In many gaming consoles, the JTAG ports are unsecured and open to user access. If you had the common interface cable for JTAG, you could plug it into your computer, use manufacturer default credentials, and play pirated games with some modifications on the attributes using the JTAG ports. The same unsecured JTAG port in an IoT device can allow an attacker to have', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 561, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9449a8b0b355ac634848c5d669f72442', 'text': 'unauthorized access and possibly have access to the private network where the IoT devices are deployed. The physical attacks, such as injecting malicious code into the IoT network, can be made possible by tampering with an IoT endpoint, gaining control over it, and then using that endpoint to gain access into the central IoT network. Attackers also exploit the JTAG interface used by manufacturers for debugging purposes. JTAG is an industry standard for on-chip instrumentation in electronic design automation (EDA). JTAG is also used to program field-programmable gate arrays (FPGAs). Most CPU vendors still use JTAG for debugging purposes. If JTAG ports are left unprotected, this interface can become a critical attack vector on the system.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 562, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67fc0f8f0987001e79b192199d5a3476', 'text': '10. Logistics is the other vulnerability in the supply chain that is prone to sabotage or modification of the IoT devices while in transit. Though this is not the most preferred attack vector for IoT devices in the supply chain, for critical infrastructure use cases, logistics needs to be carefully monitored. Your supply chain risk management (SCRM) should ensure that you have the right controls, such as choosing validated and security-cleared logistics vendors for shipping and transportation of IoT devices from production to deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 562, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9f773ccb0b555d0f1e5eafbeda19dbb7', 'text': 'The attacks are primarily aimed at data exfiltration, tampering with the files within the IoT network, and gathering information. With the control garnered over the IoT network, the attacker could control the operations and the data flow between the IoT network and the 5G network components, such as a radio (gNB) or storage/configuration in the MEC layer of the 5G network. With the control over the IoT network, the attackers can damage the IoT devices and disrupt the IoT service, thereby causing DoS to service providers’ IoT services. This is not a new threat vector for 5G technology specifically; it is prevalent in legacy technologies such as 2G, 3G, and 4G, but it’s critical for 5G technology, as it is aimed at enabling IoT use cases such as mIoT that would impact different government and private sectors.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 562, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd12a1fee953f199e950c9a0ad660bc55', 'text': 'Command-and-Control Servers and Botnets', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 562, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1210659760a9e349074fe1af5fc8742a', 'text': 'A command-and-control server (also referred to as a C&C or C2 server) is an endpoint/device that is compromised and controlled by an attacker. Devices on your network can be commandeered by a cybercriminal to become a command center or a botnet (a combination of the words “robot” and “network”) with the intention of obtaining full network control. Establishing C&C communications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 562, 'parent\_id': 'd12a1fee953f199e950c9a0ad660bc55', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '170fb448c12e32e59b2c502c0c9e234c', 'text': 'via a Trojan horse is an important step for attackers to move laterally inside service provider networks, infecting machines and servers with the intent to exfiltrate data.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 563, 'parent\_id': 'd12a1fee953f199e950c9a0ad660bc55', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e33d637c60eaf1f67ccc8783ff5c1fcd', 'text': 'One famous example of botnet malware is Mirai, which causes its infected devices to scan the Internet for the IP address of IoT devices by using a table of common factory-default usernames and passwords. The Mirai malware then logs in to the IoT devices and infects them with the Mirai malware. This method of malware infection can impact millions of IoT devices, turning them into botnets and launching DDoS attacks toward the service provider infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 563, 'parent\_id': 'd12a1fee953f199e950c9a0ad660bc55', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a5acabd0f988c876b9cfa94e014fe8da', 'text': 'Devices connected to 5G networks can implement botnet C&C protocols using a number of methods, such as Telnet, Internet Relay Chat (IRC), peer to peer (P2P), and domains, as described in the sections that follow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 563, 'parent\_id': 'd12a1fee953f199e950c9a0ad660bc55', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd7bcf8125432c7e0f6de92469136c1b2', 'text': 'Telnet', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 563, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a8af36892bede10107c53d512b505c8', 'text': 'Telnet is an application-layer client/server protocol that provides an interactive and bidirectional text-oriented communication facility using a virtual connection terminal. Telnet originated in 1969 and was specified in RFC 15, with an extended version in RFC 855, and standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 563, 'parent\_id': 'd7bcf8125432c7e0f6de92469136c1b2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ec8fd1ae212d2c2f118bbb8f4069ca1', 'text': 'Telnet, by default, does not encrypt data sent over the connection, including passwords, which makes it susceptible to eavesdropping. Authentication is also not widely used in Telnet networks, thus leading to MitM attacks aimed at using the information collected later for malicious intent. Telnet botnets use a simple C2 botnet protocol in which bots connect to the main command server to host the botnet. Bots are added to the botnet by using a scanning script, and the scanning script is run on an external server and scans IP ranges for Telnet and SSH server default logins. Once a login is found, it is added to an infection list and infected with malicious code via SSH from the scanner server. When the SSH command is run, it infects the server. The infected server is now completely controlled by the control server and becomes part of the bot network. Once servers are infected, the bot controller can launch DDoS attacks of a high volume.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 563, 'parent\_id': 'd7bcf8125432c7e0f6de92469136c1b2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '424abdcb6314bde9d213f74bb5070d82', 'text': 'Internet Relay Chat (IRC)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 563, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '33c622b3faa4ecedd3d126fbdb6986d2', 'text': 'IRC, created in 1988 and specified in the RFC 1459 standard, is an application layer protocol that works on the client/server networking model and facilitates communication in the form of text. IRC was designed for file sharing, group chats, and private chats, as illustrated in Figure 8-5.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 564, 'parent\_id': '424abdcb6314bde9d213f74bb5070d82', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '0bad2193b40e686e492a2d7c338865cb', 'text': '\\ [RC loT device server IRC loT device x ~§.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 564, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b9d9e890dd3e9de84b40aed6f024c394', 'text': 'Figure 8-5 Internet Relay Chat', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 564, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0854608314838d98760bc688a38d4ff1', 'text': 'Because of its simple and low-bandwidth methods of communication, IRC has been exploited to coordinate DDoS attacks that continuously switch chat rooms (also referred to as conversational channels or IRC channels) to avoid being', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 564, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f769ce54a10c4681ce8afa2fe8a8a6ed', 'text': 'neutralized. Figure 8-6 shows how the infected IRC devices capable of 5G can launch an attack on the 5G infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 565, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'b733c84c4dadcec2595f21e50a002452', 'text': 'IRC network infected by C&C server ! 5G capable IRC loT sensors C&C Ty \\ (A) gNB 0 2 DDoS attack = [ launched by i infected RC Centralized devices g\\B 5G Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 565, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c537ac36dc4eb64352f543632ea872f7', 'text': 'Figure 8-6 Infected IRC Devices Launching DDoS Attack on 5G Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 565, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58c96938bcaef9904e10b67b687fd2dd', 'text': 'The IRC devices can be scanned by the IRC C&C servers looking for devices that have default usernames and passwords in its list. If the 5G-capable IRC devices have factory-default usernames and passwords, they can be infected and then scan the network for other vulnerable devices. This will cause a chain reaction and impact all the devices and endpoints in the sensor network. Once the attacker is in control of the sensor network, a DDoS attack can be launched using the devices to force signaling toward the 5G network, or the data from the sensor network can be exfiltrated. Some of the malware existing today can', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 565, 'parent\_id': 'c537ac36dc4eb64352f543632ea872f7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a1a8af7c59ae8af989904e893488883a', 'text': 'also be store in the memory of the device, making it immune to mitigation via rebooting.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 566, 'parent\_id': 'c537ac36dc4eb64352f543632ea872f7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3ea51ffad131161ce673aee9003dafff', 'text': 'Peer to Peer (P2P)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 566, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '789b2623b2c2137dd0bab189297c3c09', 'text': 'P2P is a distributed application architecture that distributes tasks between peers. In a P2P network, the “peers” are endpoints (which can act as a file server and client) and are connected to each other via the Internet. The files can be shared directly between them without the need of a centralized file-sharing system, as illustrated in Figure 8-7. Hackers are now aiming IoT botnets based on the P2P network, as a majority of the IRC domains are being taken down and are no longer viable targets.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 566, 'parent\_id': '3ea51ffad131161ce673aee9003dafff', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '2201d13c9e64b107ccb96d5c79a3cd65', 'text': 'loT of¥ NetW devices p2° loT devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 566, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bb3a231e4c30dc8b14cb41d26ebee1c6', 'text': 'Figure 8-7 Peer-to-Peer Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 566, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f1f5c1b8b4e0be8cbcf5ea4d0f887a46', 'text': 'P2P technology allows lots of flexibility in consumer devices for easy access to the consumers, but it also make the devices quite vulnerable. Figure 8-8 illustrates the threat surface in a 5G network using P2P. P2P technology, if not implemented with proper authentication, can allow any potential attacker to establish a P2P connection with the device and bypass security controls such as firewalls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 566, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'afabdbc5d0c98113e18268cc7288ff4e', 'text': 'C&C [oT device infected by C&C P Infected () loT device ( A) gN\\B 0 () = = 5G ME Centralized gN\\B 5G Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 567, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '05cad0080f63a6d5ebe051fade4fd0d7', 'text': 'Figure 8-8 Infected P2P Devices Launching DDoS Attack on the 5G Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 567, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6d397f108d859e69dd2312a324a26e2d', 'text': 'Many of the IoT devices use the factory-default credentials (usernames and passwords), and the software used in these devices is quite old and mostly has no built-in security mechanisms such as authentication and encryption. The P2P communication used by many of the P2P devices is necessary for Plug and Play (PnP) features, as this offers a very simple way of deployment, without much configuration, and usually pulls a pre-filled template for Day 0 configurations from a configuration server usually deployed in the public cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 567, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '194e77079a94e9dd239cb85316701a5a', 'text': 'When such devices are deployed with 5G chipsets to enable communication with the 5G network, or if the devices communicate using non-3GPP mechanisms such as Wi-Fi and are then integrated into the 5G network, there is a high probability of attacks from such vulnerable devices. The Mirai malware has proved this attack method to be successful, as it used just the factory- default credentials to infect devices around the world.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 568, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c701377f5cbd7b1ffdc4e3bc0682f7f7', 'text': 'DNS-Based Attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 568, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '23ef0e8fb43c9a0131d9c354546de44a', 'text': 'Attacks that leverage the Domain Name System (DNS) mechanism as part of their overall attack strategy, such as cache poisoning, are considered DNS attacks. The DNS-based attack is the most scalable method used by hackers in their attempts to deploy bots that are aimed at launching DDoS attacks or causing mass-scale data exfiltration. Although this method is scalable, it is easily identified due to the large bandwidth consumption by a specific domain name. DNS blocking techniques, where specific domains are blocked, are used to mitigate these attacks. A threat surface that IoT devices could use to circumvent the DNS blocking is the Fast Flux DNS technique, as illustrated in Figure 8-9.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 568, 'parent\_id': 'c701377f5cbd7b1ffdc4e3bc0682f7f7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f7a345eeab20f3c4363ba80023186781', 'text': 'c&C Internet o loT devices [oT devices \\V v gNB (p) B3 5GMEC Centralized gNB 5G Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 569, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3a1edc38216190159e5c38ba7b89b3b9', 'text': 'Figure 8-9 Devices Impacted by Fast Flux Botnet Network Launching a DDoS Attack on the 5G Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 569, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '614532d7821271bcb057030747004821', 'text': 'To prevent the malicious control servers from being tracked down, the Fast- flux DNS technique is used by botnets. Fast-Flux DNS allows the fully', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 569, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c626ff07b9dfe0a69338c8ea36ac3df4', 'text': 'qualified domain name (FQDN) to have multiple IP addresses associated with it that are very dynamic in nature. This is made possible by the Fast-flux DNS technique, as it uses a combination of load balancing, C&C, proxy redirection, and P2P networks. The malicious control servers can also hop between DNS domains by using domain-generation algorithms that generate new domains for the control servers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 570, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b4c56808a75989f4e6eabdc33e15698b', 'text': 'Securing mIoT Deployments in 5G Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 570, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5507341f3833d2c435ec04119eed3de4', 'text': 'Mitigation of the device-based threats in 5G requires architectural strategy, rather than just deploying mitigation mechanisms for the threats from vulnerable devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 570, 'parent\_id': 'b4c56808a75989f4e6eabdc33e15698b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5dc6975d107d675de2b50baefd3e4fe1', 'text': 'The topic of mitigating the threats becomes important when there is an attack detected from the devices or when data exfiltration is detected in the service provider’s public or private cloud infrastructure due to the vulnerabilities from the IoT device. A security framework that ensures that such projects are reviewed by the security team needs to be established and (more importantly) closely followed and reviewed (at least annually). The ETSI Technical Committee on Cybersecurity (TC CYBER) has also unveiled ETSI EN 303.645, which is a standard for cybersecurity in IoT that establishes a security baseline for IoT-connected consumer products and provides a basis for future IoT certification schemes.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 570, 'parent\_id': 'b4c56808a75989f4e6eabdc33e15698b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6cae5dfa2dce68ed208437b836b066de', 'text': 'Figure 8-10 illustrates the different layers of security required to secure the IoT environment in a 5G network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 570, 'parent\_id': 'b4c56808a75989f4e6eabdc33e15698b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e166d3c6862830919c6d77f911f6d664', 'text': 'Secure Applications deployed in public cloud and on- premises', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 571, 'parent\_id': 'b4c56808a75989f4e6eabdc33e15698b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ed4424323943035953f5b3bee2458f3a', 'text': "Secure Applications deployed in public cloud and on- premises Secure communication & messages ' RBAC + Policy based access v Authentication (Token Cert... + Encryption (TLS) v Isolation & Segmentation v Authorization v Secure Zero Touch provisioning, updates & patches Secure devices v Secure Development (HW & SW) N v Hardened loT devices (secure JTAG etc) \* TPM CU., UPF, AVIF, SMF G [oT Applcations ﬂ‘\\ ; Public cloud-based MEC Authentication R ettt - - Authorization Kk Sav CU, UPF, ) AMF | SMF o= | =3 o7 Applications i e S SO —-~ On-premises MEC - - -", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 571, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cd27f7df2ae0f90402e1b5410c253330', 'text': 'Figure 8-10 Multiple Layers of Security Required to Secure the IoT Device Communication with the 5G Network Functions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 571, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9d9e5cfe9ad7d97d99d7f7eb8347d945', 'text': 'For the technical mitigation techniques, there are multiple layers of security capabilities and controls that should be put into place to ensure that the service provider’s infrastructure is secure. A lot of the security controls depend on the deployment model chosen by the service provider. This section focuses on the mitigation techniques and also provides graphical illustrations for clarity. Due', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 571, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '493c2c050a5e4d0556bd8a1396a3f617', 'text': 'to the deployment models in 5G, such as non-public/private 5G deployment, enterprise use cases are also explained in this section.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 572, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e12843cce15a6be3ca7205d381600e3f', 'text': 'Built-in Hardening of the Device', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 572, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e64e4a0f1cf559943315deb34added36', 'text': 'Service providers planning to deploy 5G devices and consumer IoT devices should ensure key built-in security capabilities are catered for, as shown in Figure 8-11 and detailed in the following list:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 572, 'parent\_id': 'e12843cce15a6be3ca7205d381600e3f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b867bd94930c81d99ffcf678f2c5dc06', 'text': '• The device provides anti-tampering functionality.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 572, 'parent\_id': 'e12843cce15a6be3ca7205d381600e3f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58b801aa1cb614ef80badb2d6d05d426', 'text': '• The device should provide a hardware root of trust.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 572, 'parent\_id': 'e12843cce15a6be3ca7205d381600e3f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7768c146b7b3a513186df11faf462a45', 'text': '• The device should support secure boot capabilities as specified by the Unified Extensible Firmware Interface (UEFI).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 572, 'parent\_id': 'e12843cce15a6be3ca7205d381600e3f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '807635ff08d0765d1b2b42ad17fd0b88', 'text': '• The hardware running is authentic, and processes are in place to protect network devices from being tainted and modified.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 572, 'parent\_id': 'e12843cce15a6be3ca7205d381600e3f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'febc2256788786b3eb05f18f225a8dc7', 'text': '• The operating system is trusted and hasn’t been modified.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 572, 'parent\_id': 'e12843cce15a6be3ca7205d381600e3f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dca53830aae1041a6731cfc8299fc08d', 'text': '• The management of the network device is properly authenticated, audited, and monitored', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 572, 'parent\_id': 'e12843cce15a6be3ca7205d381600e3f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '52aab38c5b2b1d6a10ffc22fedc466d4', 'text': '• Any secrets stored within the network device can’t be extracted or changed without proper authorization, thus providing secure data-at-rest functionalities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 572, 'parent\_id': 'e12843cce15a6be3ca7205d381600e3f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '275107dc9be78bdc6c3df9ad7d6e38da', 'text': 'Supply Chain security Protection from tampering Non-Volatile secure storage for user credentials Crypto services Verifiable source of software Secure boot process Hardware root of trust ol o Hardware protection for user information', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 573, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '73c77a5becf05c4d15cd2f59005e9314', 'text': 'Figure 8-11 Built-in Hardening of the 5G Devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 573, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '393bd9b0b008ce66382ebbf6a9154bae', 'text': 'Securing the supply chain is one of the most important topics in IoT security. This becomes more important for mIoT devices because they are manufactured with cost in mind. This leads to many IoT service providers choosing vendors and manufacturers with the lowest list price. Although this makes perfect business sense, it could lead to a disastrous consequence, with the service provider network being attacked, causing network outage, or worse, it could lead to sensitive customer information being leaked and sold to malicious entities. To secure the mIoT deployments, there should be multilayered security controls and a selection of manufacturers and vendors with secure supply chain processes.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 573, 'parent\_id': '73c77a5becf05c4d15cd2f59005e9314', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3e7dee903f587d418399d4f5ac4152c1', 'text': 'The key methods of hardening IoT devices and securing supply chain for mIoT deployments, as illustrated in Figure 8-11, are discussed further in the sections that follow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 573, 'parent\_id': '73c77a5becf05c4d15cd2f59005e9314', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6e930737d10a1f0b08880647f29196e7', 'text': 'Securing Supply Chain', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 573, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '02f4f1c27a42910eecbcd40c477fe6a0', 'text': 'Securing supply chain risks and vulnerabilities is not a new topic and has been researched for multiple industry verticals such as pharmaceutical, defense, and so on. Specific departments are often dedicated to verifying vendor selection and checking to validate that the vendors conform to regulations such as ISO9001, ICH Q10, Q9, and so on. This requires the use of approved suppliers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 573, 'parent\_id': '6e930737d10a1f0b08880647f29196e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b5774dc4da796162d79d6ffa33b91b7b', 'text': 'and a defined supply chain. Even in these verticals, however, the awareness of the subject has been historically poor and effort is lacking in the direction of securing the supply chain, unless certain leakages have been published in the media. These checks and validations are also very seldom done when IoT vendors and manufacturers are chosen by the service providers. Again, the key reason is cost; in this instance, it is cost savings by service providers to reduce the resources required to choose vendors and manufacturers. Several IoT vendors and manufacturers are working hard to improve their defense against supply chain attacks and vulnerabilities. This section will help you with some key supply chain methodologies that can then be verified against the IoT vendors and original equipment manufacturers (OEMs) you plan to use as part of mIoT deployments:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 574, 'parent\_id': '6e930737d10a1f0b08880647f29196e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6e34bc0511de84818cf57b9dfccf91d2', 'text': '• The IoT device manufacturer/vendor should have a dedicated list of supplier bases for components through which the source of the components used for manufacturing can be identified.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 574, 'parent\_id': '6e930737d10a1f0b08880647f29196e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '98053cec60136336571c875c286f668a', 'text': '• There should be strict background checks and verifications for the IoT device manufacturer/vendor employees and contractors working on the hardware and software design and development process.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 574, 'parent\_id': '6e930737d10a1f0b08880647f29196e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da118567fcc0f5d0a6dd94539f820263', 'text': '• The IoT device manufacturer/vendor should have a dedicated team with risk management training.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 574, 'parent\_id': '6e930737d10a1f0b08880647f29196e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0e1a75b5d16c0a1c9fc61863023cb3e2', 'text': '• The IoT device manufacturer/vendor should have visibility of the entire process and be able to provide you with an example of what has been done for a similar IoT device without having to expose the name of another client. In other words, there should be an identifiable process to identify the engineers and architects working on a specific IoT device manufacturing process.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 574, 'parent\_id': '6e930737d10a1f0b08880647f29196e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '575595bb8d46775ba22a7aed039f03fb', 'text': '• The schematic of the IoT device following your requirements should be verified and audited by an independent electronic design auditing organization to ensure that there is no unnecessary component design or the use of unnecessary components.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 574, 'parent\_id': '6e930737d10a1f0b08880647f29196e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d76d620e57054e476c24504aad428e2', 'text': '• Components such as chipsets used in the IoT device should not be end of life (EOL) or near EOL for at least 5 years from the date of manufacturing. You will need to work with the manufacturers for the component selection to enhance the life span of the IoT device.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 574, 'parent\_id': '6e930737d10a1f0b08880647f29196e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '08ff071ebc4f4ee137f9a9216e4a21eb', 'text': '• The IoT device manufacturer/vendor should have a software vulnerability tracking and scanning program in place as part of the software testing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 574, 'parent\_id': '6e930737d10a1f0b08880647f29196e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2c4382d8e65710923b85000d4c445956', 'text': 'process and should be able to provide you with a vulnerability report that can then be audited by an independent software auditing company. There are many instances when the software testing team sees the programs throwing up security exceptions, and the manufacturer will just ask the team to find a workaround instead of resolving the security exceptions. This will be difficult to detect. By having a report on the independent audit undertaken on the software by the manufacturer, you will have a closer view of exceptions that do not exist in the final software/firmware being deployed in the IoT device.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 575, 'parent\_id': '6e930737d10a1f0b08880647f29196e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '897c31442a1b3af647e35267458eeb3b', 'text': '• IoT device manufacturer should add a hardware security module (HSM), such as a secure element or Trusted Platform Module (TPM), on the device. Having an HSM within the IoT device will give you the ability to generate private keys and sign X.509 certificates.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 575, 'parent\_id': '6e930737d10a1f0b08880647f29196e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2674a8489d85c51092c564b57c834cea', 'text': 'Hardware Root of Trust', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 575, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '31f36f6e2ad3b64253e24ed0c030bd89', 'text': 'Having IoT devices that use signed images and hardware-anchored secure boot prevents malicious or compromised code from booting. Anchoring the first code in the boot sequence in hardware establishes a “chain of trust” and is the foundation of the secure boot process. Methods such as secure boot, which is one of the features of the UEFI specifications, is used to cryptographically verify the authenticity of the OS boot loader and the OS kernel as part of the boot process. Secure boot is commonly used to protect against BIOS rootkit attacks in server operating systems like Linux and Microsoft Windows Server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 575, 'parent\_id': '2674a8489d85c51092c564b57c834cea', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '20eccb96322f1f926f8e257b3a04c139', 'text': 'A hardware root of trust is the most important component of a hardened device. Software alone can’t prove its integrity; truly establishing trust can only be done in hardware, by using a hardware-anchored root of trust. To be effective, this root of trust must be based on an immutable hardware component that establishes a chain of trust at boot time. Each piece of code in the boot process measures and checks the signature of the next stage of the boot process before the software boots. Without a hardware root of trust, no amount of software signatures or secure software development can protect against a compromise of the underlying system.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 575, 'parent\_id': '2674a8489d85c51092c564b57c834cea', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd98fca6844687ab9bd2fac8867932f03', 'text': 'Trusted Platform Module (TPM), specified by the Trusted Computing Group (TCG) and standardized by the International Organization for Standardization (ISO) and the IEC (International Electrotechnical Commission) in 2009 as ISO/IEC 11889, is a specific processor designed to secure the hardware by using integrated cryptographic keys. Each TPM has a unique and secret', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 575, 'parent\_id': '2674a8489d85c51092c564b57c834cea', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1074115898165f95f03d0f80b36d2fa2', 'text': 'Endorsement Key (EK) assigned to it during production. This enables the primary scope of ensuring the integrity of the platform. Apart from verification of the device integrity, TPM also helps in device identification, authentication, and tamper-resistant encryption. Today, the TPMs are mainly standalone crypto chipsets and can be implemented by various device manufacturers (including consumer IoT devices) into their devices. As cost is the primary factor while manufacturing the consumer IoT devices, specific devices that are supposed to cater for 5G can be implemented with TPM capabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 576, 'parent\_id': '2674a8489d85c51092c564b57c834cea', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f1a4f5301517ad9ea0fdbce4e3a8e0f6', 'text': 'Just having TPM capabilities doesn’t mean that the devices have to be blindly trusted. As threat surfaces are always evolving and becoming more sophisticated, service providers must ensure that the monitoring of the TPM and secure boot functionalities is also taken into consideration while deploying 5G devices/5G consumer devices in the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 576, 'parent\_id': '2674a8489d85c51092c564b57c834cea', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '822dd8afcb6ab17750ed537d9fea656f', 'text': 'Some device manufacturers use Trust Anchor module (TAm), which tries to mitigate supply chain threat vectors by implementing highly secure storage for user credentials, passwords, and settings. Specifically, to mitigate supply chain attacks, some manufacturers also use the Secure Unique Device Identifier (SUDI), which is inserted during manufacturing and removes any requirement for manual intervention.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 576, 'parent\_id': '2674a8489d85c51092c564b57c834cea', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '73a0b17c0a026f9cf965d30d016220bd', 'text': 'As discussed in this section, TAm provides a permanent and secure unique identification of the device that does not require manual intervention, thus providing mitigation against supply chain attacks if implemented properly, and it can be used by manufactures in the mass-production of devices. Adoption of TAm will require a very close look at the secure manufacturing process of the vendor/manufacturer, which should follow a very stringent auditing process to ensure robust supply chain security. TPM, on the other hand, is more flexible because it doesn’t necessarily require the vendor-specific unique identifier. In turn, it provides hardware protection for user certificates and integrity information.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 576, 'parent\_id': '2674a8489d85c51092c564b57c834cea', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5262d3da6f807bb5aecb32ee863fd933', 'text': 'The most crucial point for service providers would be to verify their existing device ecosystem that has been deployed (or is planned to be deployed) and understand the threat vectors. The less hardened the device is, the more layers of isolation it requires.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 576, 'parent\_id': '2674a8489d85c51092c564b57c834cea', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '29fa8b64b7c2cc57af75cec4a492e153', 'text': 'Identification, Authentication, Access, and Certificate Management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 576, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '950a1f8dc88ad06227063f97374c4671', 'text': 'Device authentication is one of the key security controls that needs careful planning. This is because, depending on your network plans (that is, marketing team plans), the amount of mIoT devices might be in the hundreds of thousands or even in millions in a couple of years. You might even need to cater for the IoT devices that are deployed in private 5G/5G NPN networks, depending on the SLA between you and the NPN customer. Looking at the growing ecosystem of partner models for service providers using NSaaS business models, you need to ensure that there are multiple authentication layers. An example could be reauthenticating the devices in a slice using an AAA method specific for the slice, even though these device have been authenticated using 3GPP 5G primary authentication mechanisms. This all sounds simple when it’s written in a few words or shown in a figure with a few colorful boxes, but it really needs brainstorming sessions to understand the use cases and then to plan the device authentication layers. Also, you need to ensure that the device has end-to-end communication secured. If the device authentication layer is neglected or not thought through, you can spend millions in building your security architecture and still leave your network open to various attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 577, 'parent\_id': '29fa8b64b7c2cc57af75cec4a492e153', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '27c87a90c88a4c1d36b828391b2281d5', 'text': 'While discussing the topics of authentication with many service providers, one thing became very clear. There are many different types of IoT devices deployed already that support different kinds of protocols, many of which don’t even support certificate-based authentication—forget having an IPsec stack or any form of software-based authentication or hardware-based authentication/trust and so on. So, for having a pragmatic view, it is important that we have a couple of different authentication and isolation mechanisms planned for the deployed IoT devices and the IoT devices being planned for 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 577, 'parent\_id': '29fa8b64b7c2cc57af75cec4a492e153', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '38d7933b91bb7074121ea35862b1397d', 'text': 'In 5G-capable devices, for identification, the methods of international mobile subscriber identity (IMSI) and network access identifier (NAI) are used. For authentication, 5G provides at least two variants of Authentication and Key Agreement (AKA), which are 5G AKA (evolution of 4G authentication method) and EAP-AKA’ (based on the EAP). With slicing, a user device sends requests for a service to the 5G Core Access and Mobility Management Function (AMF), which is responsible for service allocation after the verification of Network Slice Selection Association Information (NSSAI). Unified data management (UDM) supports the Authentication Credential Repository and Processing Function (ARPF) and stores the subscription information and long-term security credentials used in authentication for AKA.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 577, 'parent\_id': '29fa8b64b7c2cc57af75cec4a492e153', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3e72a1403c93d1bf32118df7ed71b39f', 'text': 'The Network Slice Selection Function (NSSF) selects the set of network slice instances serving users and determines the NSSAI corresponding to applicable network slice instances.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 578, 'parent\_id': '29fa8b64b7c2cc57af75cec4a492e153', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed35a00db399f8df9fce2605d3635d8d', 'text': 'For non-5G consumer IoT devices (primarily due to cost constraints and existing legacy deployments) being served by the service provider, multiple layers of protection need to be required, such as identification verification, authentication, access, and certification management at the user, device, and application layers. Figure 8-12 illustrates authentication, authorization, and encryption for IoT devices before accessing the IoT MEC applications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 578, 'parent\_id': '29fa8b64b7c2cc57af75cec4a492e153', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '3a7619158b3dcd20a8bd0bc672682360', 'text': '[oT Application - Authentication, / Configuration, Performanc Device capable of IP, ONS Authorization & Fault Managem Encryption of APls | [oT Vendor MEC Application Infegrations with 31 party CM,PM.FM MEC Applcations APIGW Factory configured v Authentication Device ID i 0 " v Authorization 39 Party loT MEC Application v Encryption Gateway capable of A Device Authentication integration with 5G Access > ToNEF/ 5GC :TUPF A 5GoT ((A)) i Gateway 56 Acogss ! o \\ - Deployed on-premises or public loud / Device not capable of IP, DNS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 578, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a05397320bc168797bce11b2493bcf85', 'text': 'Figure 8-12 Authentication, Authorization, and Encryption Layers for IoT Devices Before Accessing IoT MEC Applications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 578, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2e57fea0eae87a6f18e9f625ec928934', 'text': 'Figure 8-12 illustrates the deployment of DNS- and IP-capable and non- capable IoT devices. The device capable of IP and DNS with 5G-capable', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 578, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8cfce210dc116a9b6203ea15ce684917', 'text': 'chipsets can use the 5G spectrum for access. The user plane (for example, API calls) from the IoT devices are terminated in the 5G UPF. The API calls from the devices are then authenticated by the API gateway (API GW) or API firewall (API FW) deployed at the public-hosted or on-premises data center.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 579, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1c85af2cda8a359ca4a135109793f960', 'text': 'The unique identity (UID), which is configured in the IoT device during manufacturing, will also be used by the device identity/device authentication layer in the IoT initial configuration by the provisioning server to verify the authenticity of the IoT device. X.509 certificate–based authentication can also be used to authenticate the IoT devices, as shown in Figure 8-13.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 579, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '485f34b8b016fea0a0fdc6232d4ba322', 'text': 'X509 CA Certificate Register and upload CA certificale 10 10T ey O0—0 —B - device authentication layer in MEC cloud [oT device Authentication Device and provisioning Database Sign certficate [oT environment MEC hosted in Public cloud loT Device | I Manufacturer Mutual Authentication of loT device & Public cloud Authentication server L L—; o I L L [ = NB On-prem / cloud Signed loT devices |oT devices deployed on deployed UPF Emergency transport', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 579, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5d1124df38af67c766af3f1339ad527f', 'text': 'Figure 8-13 X.509 Certificate-Based Authentication for IoT Devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 580, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4ca3807a2bdb5317cc2c7255d78b63ba', 'text': 'The CA certificate is registered and uploaded in the cloud-based IoT device provisioning and authentication server. The signed certificate is used by the IoT device manufacturer to sign multiple IoT devices. These IoT devices are then deployed in the emergency transport vehicle. When turned on, the IoT device installed in the emergency transport vehicle automatically connects to the pre- assigned configuration and provisioning server. The IoT device will use the X.509 certificates to perform mutual authentication with the public cloud– deployed IoT provisioning and authentication server. This is one of the methods that can be used for scalable authentication of the IoT devices. As an added security layer, a TPM could be used by the IoT device manufacturer to store cryptographic keys for authentication purpose.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 580, 'parent\_id': '5d1124df38af67c766af3f1339ad527f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '457df481db4240ef18802326d84dbef9', 'text': 'Configuration management (CM), performance management (PM), and fault management (FM) can be deployed in the cloud or on-premises data centers. Security controls related to APIs, discussed in Chapter 5, “Securing MEC Deployments in 5G,” should be followed to ensure mitigation of API vulnerabilities for any API calls between the IoT devices and the management layer or third-party applications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 580, 'parent\_id': '5d1124df38af67c766af3f1339ad527f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eca786bc76f909c26892fb262f21cb51', 'text': 'Due to the scale of mIoT deployments, the IoT authentication environment you choose should provide you with the option of identifying, provisioning, and onboarding a large number of devices based on the capabilities of the devices. Some device types have their unique X.509 certificate and private keys on them before being sold to the end customer, while others do not have the capability due to reasons such as the cost of implementing X.509 certificates and private key configurations during manufacturing.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 580, 'parent\_id': '5d1124df38af67c766af3f1339ad527f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e5faf3026158f6f4b0ea52163d489011', 'text': 'If the manufacturing chain allows the device maker to provision unique credentials into the device at manufacturing time or in distribution, the IoT authentication environment can make use of it for identification and authentication purposes. If the device does have unique certificates, then the IoT authentication mechanism, such as the assignment of temporary certificates and temporary private keys, should be used to provide initial access to the provisioning server. Once the IoT device connects to the identity and authentication management using the temporary certificates and keys, it can be exchanged with a signed unique certificate and private key.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 580, 'parent\_id': '5d1124df38af67c766af3f1339ad527f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8cb5d4373ee79778bd743391a2ea5c4f', 'text': 'Another method of authenticating the IoT devices is by using the software development kit (SDK) provided by many IoT service providers, as shown in', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 580, 'parent\_id': '5d1124df38af67c766af3f1339ad527f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ac9e8e60650e3266d116619634e4a10c', 'text': 'Figure 8-14, which illustrates IoT device integration with the public cloud using an installed SDK.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 581, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'e243387c4612ae1bbd122b7c50354362', 'text': 'loT service provider Public cloud loT with components Device SDK deployed n publc \_ Publlc cloud IoT enwronment Cloud @ L Requests from loT device to loT components deployed in cloud - ex. [AM SDK from Public Cloud provider Response from loT components deployed in loT device deployed in cloud to loT devices l T UPF 56- capable (A) [oT device On-prem / cloud deployed MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 581, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f62e2a2bfec25d590df598cfe8f6ed2a', 'text': 'Figure 8-14 IoT Device Integration with Public Cloud Using SDK', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 581, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ebd6c4c1556e83561a9c97fd0ed330e6', 'text': 'Figure 8-14 illustrates the authentication of the IoT device using the installed SDK and is explained as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 581, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd6c8bdd04fec40ffe7a905bbc3b4b011', 'text': '1. The SDK will include open source libraries. The recommended practice for low-powered devices is to use an SDK that supports device connections that use Message Queuing Telemetry Transport (MQTT). The SDK will include a basic set of functionalities and policies to access the cloud-based IoT provider.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 581, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '91cce17b92b326e4a1d0e6d946285db3', 'text': '2. The key functionalities of the IoT service provider are deployed in the cloud. One of the key components is Identity and Access Management (IAM), which is used for authenticating the IoT devices. The API gateway (API GW) is used to protect the IoT applications from API vulnerabilities, such as providing rate-limiting functionalities and enhanced authentication and authorization functions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 582, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f62704b930161ea7174b13f7f47fd764', 'text': '3. Installing SDKs in the IoT devices will help you integrate IoT products to your choice of IoT providers deployed in public cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 582, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '92820eb85d5e618315bfa9d9d04ff201', 'text': '4. The SDK deployed within the IoT device will initiate an HTTPS request towards the authentication, authorization, and accounting (AAA) component of the cloud-based IoT provider. The HTTPS request includes the X.509 certificate, which is verified by the AAA component to authenticate the IoT device.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 582, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8325c3cec3245ce338ae3fc837bbf163', 'text': '5. Once the mutual authentication is performed, initial configuration can be downloaded to the IoT device. One of the other functions that can be performed is to attach a policy for the device, such as allowing the device to connect to the analytics engine, enabling you to enhance the services being offered to the IoT use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 582, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2dd09cd547b3f74a87684dd5e9ab909d', 'text': 'In pragmatic deployment considerations, you also need to consider integration of hundreds of thousands or even millions of devices, which might require AAA to be deployed in the public cloud, as illustrated in Figure 8-15.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 582, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c01b9a0581ee811cfdfcaf9bc5c765dc', 'text': 'Cloud CM, PM, FM for [oT devices based AAA SP Applications & Data Network CPNFs % UPF o= ssssssssssssns = v ssssssssnnsans Centralised 5G Core IJ.. 5G MEC ((A)).\_. -0', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 583, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '272689c4e4cd2316b78b04726e63252a', 'text': 'Figure 8-15 Cloud-Based Authentication for IoT Devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 583, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c01cc8e53a3d51f7064866cf452bfedc', 'text': 'One way to tackle the issue of identifying millions of devices is to build a strategy around having a unique ID (UID) assigned during the manufacturing process that can be used to identity and authenticate the device. Having a unique ID will also allow service providers to have proper lifecycle management, including tracking the software and hardware changes. Any infection or abnormal behavior can be easily tracked down to a specific device or group of devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 583, 'parent\_id': '272689c4e4cd2316b78b04726e63252a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '015b903fdaa4000c393f1a49cfd1e543', 'text': 'Network Slice Isolation and Segmentation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 583, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '75e7d1392b9fa0118072baeeaf571a66', 'text': 'Network slicing is one of the key evolutions of the network deployment brought in by 5G technology. Network slicing is the ability of the network to (automatically) configure and run multiple logical networks as virtually independent business operations on a common physical infrastructure. Network slicing is a fundamental architecture component of the 5G network, fulfilling', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 583, 'parent\_id': '015b903fdaa4000c393f1a49cfd1e543', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f08f036ad84be7716d30f0e2abc87632', 'text': 'the majority of the 5G use cases. Many operators are considering the offer of a network slice per enterprise, which is not that dissimilar to the per access point name (APN) offer for an enterprise in play today. As we consider the points where the enterprise then touches the 5G slice, a number of security aspects must be addressed—one of them being slice-level isolation, as illustrated in Figure 8-16.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 584, 'parent\_id': '015b903fdaa4000c393f1a49cfd1e543', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '7b506c0896e41d937ef4b01a3478462d', 'text': 'Slice 1 AUSF UDM PCF NEF g UPF SMF- AMF Slice NFs Slice 1 f— deployed in J—— separate servers s SP Subscribers ((A)) AUSF UDM PCF NEF lice Slice 2 Enterprise Network MEC Application UPF SMF AMF = ] \\ Enterprise serving loT devices with dedicated RAN, UPF and Control Plane NFs for Enterprise Slice MEC applcations on premise deployed in senvice provider 5GC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 584, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7f4eab488a543669c8b88201d9ed3b6b', 'text': 'Figure 8-16 Slice Isolation and Segmentation for IoT Devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 584, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a9f88686aef46403e9f5b8c30a2e5868', 'text': 'Network slicing architecture, which allows the ability to run multiple logical networks as virtually independent business operations on a common physical infrastructure, also requires high isolation between the slices. Isolation within', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 584, 'parent\_id': '7f4eab488a543669c8b88201d9ed3b6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '57b6a64204ef365be83225759b51db41', 'text': 'the components of the slice prevents the vulnerabilities from spreading to other components within the slice and between the slices in the case of any malicious attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 585, 'parent\_id': '7f4eab488a543669c8b88201d9ed3b6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd19cd6c8b73b7bfde588d01ad01b068e', 'text': 'Intra-slice and inter-slice isolation should be implemented for both public and non-public networks (NPNs). The network slices should also allow a quarantine slice for identified malicious hosts, which provides isolation and restricts the spread of malware due to lateral movement.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 585, 'parent\_id': '7f4eab488a543669c8b88201d9ed3b6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'be09b608c346eba18fa62dcc6410d803', 'text': 'Intra-slice can be provided by ensuring that the CNFs serving the slice are deployed on separate hosts. This ensures high availability for the slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 585, 'parent\_id': '7f4eab488a543669c8b88201d9ed3b6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a233db3651a75f5f9e32c6c4756fad82', 'text': 'Inter-slice isolation can be provided by deploying 5GC CNFs on separate hosts and then implementing network segmentation between slices. This mitigates malware propagation between slices of different sensitivity, such as a slice serving critical infrastructure (considered a highly sensitive slice) and a slice serving IoT devices (considered a less sensitive slice).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 585, 'parent\_id': '7f4eab488a543669c8b88201d9ed3b6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '72dfbcab1203d48b37e6eac92b512d4d', 'text': 'Segmentation and isolation mechanisms used for the IoT deployment will vary depending on your deployment mode to cater for the mIoT use cases. If network slice mechanisms are used to provide access to the IoT device, you should ensure that the 3GPP 5G functions are isolated from other slices. This can be done by using separate x86 servers for deploying mIoT slice NFs. You should also architect your network such that web-facing applications are in a separate security zone and are not deployed in the same x86 server. This will ensure physical separation of the NFs and will reduce the probability of any side-channel attacks exploiting the vulnerability of the host OS and hardware (HW). If the mIoT devices are being deployed in the NPN network, then you should ensure that you have the mIoT network and the operational technology (OT) completely isolated from your IT network using a demilitarized zone (DMZ). In fact, if the mIoT is being deployed for critical use cases, there should be integrations with the IT network only if it is really necessary. Remote access to such networks should follow stringent identity and access mechanisms and should be continuously audited. This could be done by using a next-generation firewall (NGFW) integrated with your Network Access Control (NAC) and IAM layers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 585, 'parent\_id': '7f4eab488a543669c8b88201d9ed3b6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bfb5d233f36f9585e6d49349cdd313ba', 'text': 'Securing network slices is covered in detail in Chapter 7, “Securing Network Slice, SDN, and Orchestration in 5G.”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 585, 'parent\_id': '7f4eab488a543669c8b88201d9ed3b6b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7855c5edf5b14ecaf4bff45dfb9bb139', 'text': 'Mitigating IRC and P2P-Related Attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 585, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f2032c3e960e3c9932add5a6b48c4ec2', 'text': 'In general, deploying IRC and P2P IoT devices in the subscriber’s location should be avoided. But pragmatically speaking, it is well known that the security team of the service provider is rarely informed of IoT devices being sold to customers by the customer-facing teams of the service provider. To solve this issue, recommended practice dictates that service providers check the type of device, secure the development lifecycle followed by the device manufacturer, and look at the supply chain lifecycle of the device manufacturer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 586, 'parent\_id': '7855c5edf5b14ecaf4bff45dfb9bb139', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ad2fdfe8d8189dd11a6dd1a512a9d617', 'text': 'If the existing devices within the service provider use IRC, then in cases of IRC-related botnet attacks, each bot client must know the IRC server, port, and channel. Anti-malware solutions available today can detect and shut down these servers and channels, effectively halting the botnet attack. If this happens, clients are still infected, but they typically lie dormant since they have no way of receiving instructions. A botnet can also consist of several servers or channels. If one of the servers or channels becomes disabled, the botnet simply switches to another. It is still possible to detect and disrupt additional botnet servers or channels by sniffing IRC traffic, which can be catered for by anti- malware and monitoring solutions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 586, 'parent\_id': '7855c5edf5b14ecaf4bff45dfb9bb139', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1a63baeb7eb616dfe95147b5a0eb718e', 'text': 'If the existing devices within the service provider use P2P, for mitigating the P2P attacks that use the firewall pin-holing technique, then granular firewall configurations to block traffic on specific ports should be used. This would prevent infected devices from communicating with the malicious P2P servers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 586, 'parent\_id': '7855c5edf5b14ecaf4bff45dfb9bb139', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9494db3e3f18570f116dbe3307474b3c', 'text': 'Zero-Touch Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 586, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fa733c32851aaf1bf2601e32cbae600f', 'text': 'Many of the consumer devices aimed at enabling IoT use cases use Zero Touch Provisioning (ZTP) to allow the PnP capabilities. This is done to allow easier deployment for the customer and provide a better user experience. Before choosing such devices from a manufacturer or vendor, the service provider should check whether the device manufacturer or vendor uses ZTS as a model for the ZTP process. Depending on the vendor, the method of ZTS is also called secure zero touch or zero touch secure identity, or other variants.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 586, 'parent\_id': '9494db3e3f18570f116dbe3307474b3c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '427c484f78b8a2f88ec1959d9c38f10c', 'text': 'Implementing ZTS by the device vendor is quite critical, as it secures the device and authenticates and encrypts its communication with the cloud-hosted provisioning and configuration server or PnP servers and provides a secure lifecycle thereafter, including secure auto-deployment of patches, secure auto- installation of updates, and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 586, 'parent\_id': '9494db3e3f18570f116dbe3307474b3c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e0e7d9bb89ae3f735a42b8d6879ced6d', 'text': 'ZTS techniques used by the vendor should also ensure continuous authentication if any anomaly in behavior is detected or if reauthentication of the device occurs at certain intervals without interrupting the device functions. During assessment of the device vendor by the service provider, scalability of the solution should also be verified. Quite a few vendors in the market today use artificial intelligence (AI) to detect anomalies in behavior and can initiate the detection and response capabilities automatically depending on the behavior of the devices, including triggering the reauthentication of the devices and moving the devices with anomalous behavior to an isolated segment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 587, 'parent\_id': '9494db3e3f18570f116dbe3307474b3c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '59146e85d76b64f1217ea9a4ffcdbf9e', 'text': 'DNS Security for 5G IoT Devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 587, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '707d707511bca6c1e1060fb4e73a642e', 'text': 'The Domain Name System (DNS) plays a very important role in the IoT ecosystem. The 5G devices enabling consumer IoT would primarily be using cloud-based provisioning servers for PnP, which is usually configured using an FQDN that will have the URL of the provisioning server configured or hardcoded. Using this configuration, the device will connect to the provisioning server, get authenticated (depending on the device vendor), and then connect to cloud services to transmit and receive data.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 587, 'parent\_id': '59146e85d76b64f1217ea9a4ffcdbf9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5c6badf3232feea03e00aff27f651685', 'text': 'One of the key threats is DNS cache poisoning attacks, where a malicious or fraudulent IP address is logged in the local memory cache. The device configuration can also be modified for it to connect to a malicious server. This is because the devices trust the domain names to be secure. If an attacker changes the original domain name within the configuration template of the device or can change the hardcoded domain name to a malicious one, the device will try connecting to that domain name. The attacker can then insert a rogue update to the device, potentially taking full control of the device and targeting it against the service provider infrastructure, causing a DDoS attack or taking down the infrastructure, causing a DoS attack.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 587, 'parent\_id': '59146e85d76b64f1217ea9a4ffcdbf9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0e4b0902460611a6667f189f30d49cea', 'text': 'DNS, although scalable, does not include any inherent security mechanisms such as encryption, which makes it vulnerable to MitM attacks for interception and manipulation. Domain Name System Security Extensions (DNSSEC) and DNS over HTTPS (DoH) improve the security capability of DNS. DNSSEC is becoming more important for IoT devices due to the fact that it secures parts of the supply chain system as well. When an IoT device is manufactured, many of the device vendors use the cloud-based configuration for shipping and initial factory configuration. This is because many of the orders from service providers can be customed labelled so that when the customers receive their', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 587, 'parent\_id': '59146e85d76b64f1217ea9a4ffcdbf9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e5298fc56e7a3c42078d0693a5c02e0b', 'text': 'devices, they will be in the name of the service provider. This requires some changes at the manufacturing end, and many of these processes are automated in the industry these days. Secure DNS solutions can also be used by the service providers to enhance security for the IoT devices. This is further explained in detail in this section.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 588, 'parent\_id': '59146e85d76b64f1217ea9a4ffcdbf9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '02e318c88b7206e5042a2b0cd3b8e6e2', 'text': 'DNSSEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 588, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2ddfa6fff1fbe0053f8505000dc87338', 'text': 'DNSSEC is a set of extensions to DNS that provides a security chain of trust and protection from DNS vulnerabilities. DNSSEC provides DNS clients with cryptographic authentication of DNS data by using cryptographic keys to validate connections between the DNS client and a domain name.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 588, 'parent\_id': '02e318c88b7206e5042a2b0cd3b8e6e2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ee8a62a9031dc308d046e2daa311989', 'text': 'Having DNSSEC as part of the device capability will ensure that the device is routed and connected to the authentic server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 588, 'parent\_id': '02e318c88b7206e5042a2b0cd3b8e6e2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '692a2e5d9b1bf6015456b97ec34f7e3c', 'text': 'Although DNSSEC adds integrity and trust to DNS, it does not provide confidentiality (DNSSEC responses are authenticated but not encrypted), which means that the DNSSEC responses can be intercepted. As the attacker can attempt to use DNSSEC mechanisms to consume a victim’s resources, it does not provide complete mitigation against DoS attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 588, 'parent\_id': '02e318c88b7206e5042a2b0cd3b8e6e2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ef2f594170c999b5691e06e7bb84dff7', 'text': 'DoH', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 588, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '650bd58eef140a9fe95358688522913a', 'text': 'DNS over HTTPS (DoH) caters for DNS resolution using the HTTPS protocol. Using HTTPS, DoH provides better user privacy and prevents MitM-type attacks because it includes encryption between the DoH client and the DoH- based DNS resolver. DoH is published by the IETF as RFC 8484.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 588, 'parent\_id': 'ef2f594170c999b5691e06e7bb84dff7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f8e36215509a096f5ec88df838af595d', 'text': 'DoH works just like a normal DNS request, except that it uses Transmission Control Protocol (TCP) to transmit and receive queries. DoH takes the DNS query and sends it to a DoH-compatible DNS server (resolver) via an encrypted HTTPS connection on port 443, thereby preventing third-party observers from sniffing traffic and understanding what DNS queries users have run or what websites users are intending to access. Because the DoH (DNS) request is encrypted, it’s even invisible to cybersecurity software that relies on passive DNS monitoring to block requests to known malicious domains.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 588, 'parent\_id': 'ef2f594170c999b5691e06e7bb84dff7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0f57fae243bcb89b8c133d094619e287', 'text': 'If service providers plan to use DoH-based endpoints, there are certain mechanisms the security team can put into place to ensure that the devices use specific browsers. Browsers such as Chrome ensure that DoH will only be', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 588, 'parent\_id': 'ef2f594170c999b5691e06e7bb84dff7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd0cce61013cc1cd416885f2e368c4012', 'text': 'enabled when system DNS is observed to be a participating DNS provider. After DoH is enabled in Chrome, the browser will send DNS queries to the same DNS servers as before. If the target DNS server has a DoH-capable interface, then Chrome will encrypt DNS traffic and send it to the same DNS server’s DoH interface.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 589, 'parent\_id': 'ef2f594170c999b5691e06e7bb84dff7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '435316914304a6e435c7d151a8440e66', 'text': 'Secure DNS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 589, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e7913f4d7a5f4676e32f87ca80ff8d0c', 'text': 'In many cases, consumer IoT devices today are not yet fully DNSSEC or DoH capable. One of the mitigation mechanisms from DNS cache poisonings and malicious DNS configurations is to use a cloud-based DNS security layer that ensures that the DNS request is not resolved to a malicious domain. There are vendors in the market today that integrate the secure DNS resolution along with the threat intelligence, anti-malware, and antivirus capabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 589, 'parent\_id': '435316914304a6e435c7d151a8440e66', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6a18babffc8a0e0a2e07d3480dfd9c6f', 'text': 'As illustrated in Figure 8-17, when the DNS security layer receives a DNS request from a 5G-capable IoT device, be it for the provisioning or PnP layer or for CM, PM or FM, it should use threat intelligence to determine if the request is safe, malicious, or risky—meaning the domain contains both malicious and legitimate content. Safe and malicious requests can be routed as usual or blocked, respectively. Risky requests can be forwarded to an inspection layer for deeper inspection. The secure DNS layer should also inspect the files attempted to be downloaded from the sites using antivirus (AV) engines and anti-malware protection, and based on the outcome of this inspection, the connection should be either allowed or blocked.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 589, 'parent\_id': '435316914304a6e435c7d151a8440e66', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c702558e2daea8d1b62424f3839fc78d', 'text': 'DIA (Direct Internet Access) for PnP I Zero Touch day 0 config / stats collection for PM /FM — ) CMPM,FMfor loT devices 5GMEC S Secure DNS Applications% ta SP Applications & Data Network e CI P L R CPNs L[ | !00 ( A)) o % UPF S — g — | O Centralized 5G Core - o= ] 5G MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 590, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1d642e80a539f046f53e46bbdaf1b9b9', 'text': 'Figure 8-17 Securing DNS Layer Communication of IoT Devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 590, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c1981a7508a37a73878fdcfd921ce108', 'text': 'This is one of the most effective methods that will lead the security teams to remediate fewer instances of malware, and the threat is mitigated even before the devices are impacted or an attack is launched. Service providers selecting vendors or partners for secure DNS solutions should ensure that they have extremely good threat intelligence to ensure high efficacy. They should also ensure that the vendor providing such solutions has a robust machine learning algorithm that allows the solution to predict attacks. Many of the recursive DNS service providers resolve millions if not billions of Internet requests every day, and they have ML algorithms analyzing the massive amount of data to understand patterns and co-relate patterns by running statistical and machine learning models to identify attacks and thus uncover the attacker’s infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 590, 'parent\_id': '1d642e80a539f046f53e46bbdaf1b9b9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b76a066ccc77032ee94ee5c23768b45a', 'text': 'The secure DNS layer is also easy deployable and doesn’t have any requirements on the device itself. It only requires the DNS IP address to be changed from a previous DNS IP address to the secure DNS provider’s IP address. Any DNS request coming from the device will now be redirected to', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 590, 'parent\_id': '1d642e80a539f046f53e46bbdaf1b9b9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6b6c7c6f2990ee4d885178ef2986ff43', 'text': 'the secure DNS vendor’s cloud network, which will then resolve all the DNS requests and block any request to the malicious domains.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 591, 'parent\_id': '1d642e80a539f046f53e46bbdaf1b9b9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5e12767760f2dcda8d6d6096c858649c', 'text': 'Enhanced Visibility and Monitoring', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 591, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a5031bb64fbacbd03ef7a3d71382fd6', 'text': 'One of the most important security capabilities that’s required in any organization is enhanced end-to-end monitoring to understand the communication among the devices and between the devices and the network elements, including monitoring the encrypted traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 591, 'parent\_id': '5e12767760f2dcda8d6d6096c858649c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7fbda8c141f4add8e99ac2571cd62576', 'text': 'After discussing and deploying proof of value (PoV), which is a marketing term used by many vendors to make solution validation in service provider networks sound cooler, a number of service providers see very little value in aggregating and tapping the user plane data of the devices. In 5G, the user plane data from devices (eMBB slice-related devices) will be in the terabytes pf volume. Having a solution for end-to-end user plane (UP) monitoring is not viable due to cost and technical reasons. Control plane, service plane, and OAM are the key layers that should be monitored at minimum. By validating this method in multiple service providers, it is quite clear that many of the anomalies can be detected by monitoring the control plane, service plane, and OAM layer. Once the monitoring for these layers is established, the service provider can pick and choose the UP-layer visibility for specific use cases. IoT devices (related to machine-to-machine use cases), as such, are not user plane intensive, so having granular visibility would not be a major hurdle in terms of cost.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 591, 'parent\_id': '5e12767760f2dcda8d6d6096c858649c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '27b4c9c6c22b7342c9b778481bb85e7d', 'text': 'Before investing in an end-to-end monitoring system for the consumer IoT, service providers should try to build a unique ID system, as explained in the section “Identification, Authentication, Access, and Certificate Management” in this chapter. This will also help the service providers in reducing the mean time to repair (MTTR), as the service provider can quickly respond to the unplanned device breakdown.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 591, 'parent\_id': '5e12767760f2dcda8d6d6096c858649c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9e48b52855c17c9d0ccf44c54f4c34aa', 'text': 'Figure 8-18 illustrates the monitoring system for anomaly detection for your deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 591, 'parent\_id': '5e12767760f2dcda8d6d6096c858649c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'e5957d95215ed28b65729c822577989c', 'text': 'v v \\} v Anomaly Detection Engine & Corrective action Data Collection —» Palch management Hypervisor Metadata, Container Telemetry, NSEL, NetFlow, IPFIX 0 Slice 1 AUSF UDM PCF NEF f UPF SMF - ANF Slice NFs Slice 1 \\ deployed in ssssesen separate Host F———— HW & Sw .8 ((A)) SP Subscribers AUSF UM PCF NeF @ Slice 2 Slice 2 Enterprise Network MEC Application UPF SMF - ANF = s', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 592, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9ab0f257cab7f90bd19df54349a9f3cf', 'text': 'Figure 8-18 Enhanced Visibility of IoT Device and IoT Slice Layers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 592, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bb47c97661b4a3bb4550af4d0dccd99e', 'text': 'As shown in Figure 8-18, the monitoring solution should also cater for enterprise use cases, as 5G allows easier integration into the enterprise networks using methods such as multi-access and edge computing (MEC) and network slicing. Due to the flexibility in deploying the use cases, the monitoring solution should also follow flexibility and scalability. There are', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 592, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0195cacf1bd18884eb5a6a3266229455', 'text': 'monitoring solutions available in the market today that allow for multivendor packet flow collection (without the need for physical probes) and then analyze the data collected after packet de-duplication and VXLAN striping. Having such monitoring solutions would also support other use cases, such as reusing the same solution for IT and telco DC infrastructure monitoring.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 593, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd4148decde6de960f8928fd2698f9d31', 'text': 'It is also recommended that you look at utilizing monitoring solutions that have integration with the products with capabilities such as responding to any detected anomalies within the device or the device network. The minimum possible response should be the capability to isolate the infected devices or push the devices into a segment that will have access to only critical services.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 593, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9951ea65f12577df667df4bab9e6e3ec', 'text': 'The visibility and monitoring layer, though very critical, might become very expensive for you if you don’t plan it properly for the IoT use cases. One of the methods you could use here to optimize is to consider enhanced visibility and monitoring for control plane, service and management layer of the network functions, and network devices specific to the IoT network. If the IoT network and devices use API-based communications that are encrypted using Transport Layer Security (TLS), it is important to have visibility in the encrypted layer as well. Using a decryption engine and then analyzing the packets, though effective, is not always the best method, as multiple decryption points will reduce the effective security posture of your network. In such cases, it will be more effective to perform malware detection in encrypted traffic without decryption using solutions available today that analyze the encrypted packet header and look at the behavior of cipher suites and so on to determine any anomaly and malicious behavior. Some smart mIoT devices will also provide a basic telemetry with a couple of key counters, which will help you to understand if they have been tampered with. Such IoT devices can be blocked or reported to the IoT device user, depending on the SLA.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 593, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a2311bc4da364a2d2fac6590a1e5f186', 'text': 'Access Control', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 593, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2812a907a6b8a0be9fdb96802b86469a', 'text': 'Access control for 5G SIM or universal integrated circuit card–capable devices are catered for by the inherent 5G Identity and Access Management mechanisms. But many of the consumer IoT devices being deployed for quite some time will use non-3GPP technologies and legacy 3GPP mechanisms and connect to the 5GC using network elements like the non-3GPP Inter-Working Function (N3IWF), which is responsible for the interworking between the untrusted non-3GPP components and the 5GC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 593, 'parent\_id': 'a2311bc4da364a2d2fac6590a1e5f186', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '48543f195d8d0af7c0f82efc41e8b3a0', 'text': 'There are various access control mechanisms used by service providers today, primarily role-based access control (RBAC), mandatory access control (MAC), access using security group tags (SGTs), attribute-based access control (ABAC), and so on. For the cloud-hosted IoT management functions such as CM, PM, and FM and provisioning servers catering for consumer IoT devices, a very strict RBAC schema should be applied as a minimum, which is then followed by using multifactor authentication (MFA) for the users and devices. There should be layers of access control for any remote configuration of the IoT subsystem (controller, server, device, and so on).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 594, 'parent\_id': 'a2311bc4da364a2d2fac6590a1e5f186', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aca93c45442d30c88bb8de1cb3daed2d', 'text': 'To ensure that only legitimate users with the right levels of access are accessing the management layer/operational technology (OT) of the IoT network, you should apply zero-trust principles and use mechanisms where you authenticate and re-authenticate the users at varying levels of time and network layers. For example, you should use mechanisms such as MFA, which is integrated into your existing Identity and Access Management (IAM) layer. This integration will ensure that any change in the user’s role is mapped to RBAC. If the previous role of the user was admin with privilege access, once the person leaves the organization or changes role, the integration will ensure that the person does not have privileged access anymore. This layer, although foundational, is rarely designed properly due to multiple access control vendors and multiple MFA vendors being deployed at different departments of the service provider. In some cases, there are six to seven multiple IAM solutions deployed in the same domain of the service provider, thus unnecessarily complicating the access control and leading to improper configuration and blind spots.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 594, 'parent\_id': 'a2311bc4da364a2d2fac6590a1e5f186', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5095053eb9995d26bc001ad04ca89336', 'text': 'Figure 8-19 illustrates the granular access control for IoT deployments by providing the secondary authentication mechanism for IoT devices using the enterprise AAA/IAM.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 594, 'parent\_id': 'a2311bc4da364a2d2fac6590a1e5f186', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '8b0349f8317d550cf6957e4fc5323757', 'text': '— AAA in Network Slicing — AAA for secondary authentication Enterprise AAA 1AM used for device —~0 authentication N6 5G MEC Applications & Data Network NSSAF | AAAP PP AMA/ UPF UPF deployed in A Enterprise Network e ? AMF SMF & ssssssassassssasansnaa: Seessssscecsssacnenana.. ((A)) Enterprise Network NB Centralized 56 Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 595, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '98c6691900add10e2b231377dcc90131', 'text': 'Figure 8-19 Granular Access Control for 5G IoT Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 595, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ea2062622d871317c869fbf66261953a', 'text': 'As shown in Figure 8-20, the user will have to go through primary authentication, secondary authentication, secure Internet access, and a granular role-based access for accessing the device and the consumer IoT subsystem.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 595, 'parent\_id': '98c6691900add10e2b231377dcc90131', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '108c5e64682cd27bed44adfec6c94ea8', 'text': 'I 10 ©% 2 o i Employee Contractor Secure intemet Primary Secondary RBAC - Role based HW & SW Vendors access Authentication Authentication access control HW & SW Sub-contractors - R e S e e o " /X " e e e e e R e A R e e e e e e e e e e e e e - 5G MEC Applications CM, PM, FM for l—’ %@ loT devices SP Applications & Data Network s | : w [ — [ ——— o= \'JOO ‘—\'\_ (=] Centralized 5G Core 5G MEC L+ ) ——/ S —', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 596, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9859896f71fda211fc1beea0d25d5541', 'text': 'Figure 8-20 Granular and Multilayered Access Control for 5G IoT Network and IoT Devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 596, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c9752ffef4bf9adc121090a877d8ea5d', 'text': 'DDoS Protection', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 596, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '57ed22bf27951872be94ff7805c9b8bb', 'text': 'One of the key threat surfaces in 5G-capable IoT devices is DDoS, due to the sheer number of devices (both low bandwidth and high bandwidth) expected in', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 596, 'parent\_id': 'c9752ffef4bf9adc121090a877d8ea5d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '74dbd5f89a7c10ac02c5ae2f18ba9179', 'text': 'the service provider’s infrastructure in 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 597, 'parent\_id': 'c9752ffef4bf9adc121090a877d8ea5d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '82255476978a41b1b636481c3b2955e5', 'text': 'Looking at the growing sophistication of DDoS malware, service providers need to implement the most sophisticated security solutions to protect against new threats and emerging attack types. Attackers are deploying multivector attack campaigns by increasing the number of attack vectors launched in parallel. To target an organization’s blind spot, different attack vectors target different layers of the network and data center. Even if only one vector goes undetected, then the attack is successful, and the result is highly destructive. Attacks are becoming completely automated and more sophisticated, making it difficult to defend against them manually. New techniques like burst attacks and advanced persistent denial-of-service demand advanced detection and mitigation and underscore the need for automation. Figure 8-21 illustrates the location of the anti-DDoS solution to mitigate DDoS attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 597, 'parent\_id': 'c9752ffef4bf9adc121090a877d8ea5d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ee65bc106518e2918ef7f5ffd5b5eed7', 'text': "DDoS Protection G MEC Apphcat\\ons SP Applications & Data Network CP NFs w ( ) % UPF o= 'JOO \_ \_ NB Centralized 5G Core 1 5G MEC Enterprise Network o MEC Application (A) @,—", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 598, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e4c84d55d9de78afe9f093680be0c151', 'text': 'Figure 8-21 DDoS Protection for the 5G IoT Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 598, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '90e54d4fa1b53801b745786666e393ca', 'text': 'There are anti-DDoS mechanisms available in the market today that can detect the DDoS attacks by analyzing the packet flows and then taking the decision to drop the packets if they are identified as part of the DDoS attack. The DDoS protection solution would normally create baselines of a normal network, application, and user behavior and use these baselines to notice abnormal traffic and accurately detect attacks. When a new, previously unknown zero- day attack is detected, the solution creates a signature that uses the attack characteristics and starts blocking the attack. The mechanism described is true for any technology and for 5G. But in 5G the deployment of the anti-DDoS solution need not be deployed at the centralized 5GC layer but can instead be', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 598, 'parent\_id': 'e4c84d55d9de78afe9f093680be0c151', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ced085067141a674d2e5106a7465a75c', 'text': 'deployed at the MEC or distributed DC layer. This ensures that the DDoS packets are mitigated at the edge of the network and do not hog the back haul.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 599, 'parent\_id': 'e4c84d55d9de78afe9f093680be0c151', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '339c41f293999bf55f6a89e22e00e152', 'text': 'Using a next-generation firewall (NGFW), anti-malware, and DDoS protection functions is not new for 5G and has been part of the security ecosystem for quite some time. Although the functions have not changed, the type of deployment and the features required within these functions needs enhancement to cater for the mIoT and other 5G use cases. One of the key changes is the container-based deployment of 5G functions, which means that a single IP address could have multiple NFs; this requires the application-level microsegmentation and access controls to be implemented. This should also cater for identifying vulnerabilities in the open source Cloud-Native Functions, which are the norm for 5G 3GPP NFs. Developers of non-3GPP-based 5G NFs aimed to be deployed in the MEC Layer are also building their applications using open source software.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 599, 'parent\_id': 'e4c84d55d9de78afe9f093680be0c151', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3d5aa2bc111c6f05607fccbcc82d33db', 'text': 'Real Scenario Case Study: mIoT Threats and Their Mitigation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 599, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f4a3c19ea04aa77a08811d447461ecfb', 'text': 'This section focuses on a real scenario case study of attacks from threat vectors in a 5G mIoT environment and discusses techniques for threat mitigation. Although 5G was not widely deployed at the time of writing this book, this section is based on real-life attacks in similar environments or proof of concepts and lab tests done by various customers. This section will take you step by step through malware infection of the device and then explain a mitigation technique.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 599, 'parent\_id': '3d5aa2bc111c6f05607fccbcc82d33db', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '939d8bc8628cedca180343db3353ebc6', 'text': 'Figure 8-22 shows the 5G IoT network used as the example for the attack scenarios discussed in this section.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 599, 'parent\_id': '3d5aa2bc111c6f05607fccbcc82d33db', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'bd080277ba479f2a943760e0024e1205', 'text': "DIA (Direct Internet Access) for PnP / Zero 5GMEC CM, PM, FM Touch day 0 config / stats collection for PM /FM Apphcanons IoT devices \\ 1 SP Applications & Data Network ba - [EpRR R . w - 'J'OO J W—a \_ [ =] gNB L ) L 5GMEC Centralized 5G Core", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 600, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '95c1be007ed16175df60556569f307f6', 'text': 'Figure 8-22 5G Network Serving IoT Devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 600, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1e3235959bd67eec9b3e3eb46e42254a', 'text': 'Figure 8-22 illustrates IoT devices that are connected to the IoT applications and management components, such as CM, PM, and FM, deployed in the cloud. The IoT devices are configured using a domain configuration that lets you specify a custom FQDN to connect to the public cloud IoT environment. The FQDN is configured using the CM deployed in the cloud. The IoT devices are factory-configured to resolve to a preconfigured server (IP address/URL). Once the IoT device resolves the URL to the PnP server, the initial custom configuration is then downloaded to the IoT device, which includes the details for configuration, performance, update servers, and patch servers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 600, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0722212d22eb81910db3b6294d610e15', 'text': 'Threats Example', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 600, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f8cd4aa578482ca26894696d924ccadf', 'text': 'In Figure 8-23, the consumer IoT devices connect to the Internet and discover the provisioning server based on the FQDN attributes provided by the CM of the IoT device. In step 1 of the threat, the CM is exploited by a vulnerability.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 600, 'parent\_id': '0722212d22eb81910db3b6294d610e15', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ead6eb34fd4b4c292efe60261a9bad38', 'text': "5GMEC CM, PM, FM DIA (Direct Internet Access) for PnP Apphcanons IoT devices | Zero Touch day 0 config/ stats collection for PM / FM [ SP Applications & Data Network ba - [ R . w [RpRR R 'J'OO J W [ -] \_ gNB = 5GMEC Centralized 5G Core L )", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 601, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '04c739fb70bd1dfc37d7f5d702e7571f', 'text': 'Figure 8-23 IoT Configuration Management Vulnerability Being Exploited', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 601, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '07ac6a47b3d6d6023fe637fc5beeb8c7', 'text': 'Figure 8-24 illustrates the IoT device FQDN being modified by the attacker.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 601, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'e54b77e34fd5a8762a24739b8aee642b', 'text': 'DIA (Direct Internet Access) for PnP / Zero 5G MEC CM, PM, FM for Touch day 0 config / stats collection for PM Apphcatuons IoT devices 1 \_ SP Applications & Data Network ba w [ ——— [ R ——— i@ IJ.. R — [ =] g\\B - L 5G MEC Centralized 5G Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 602, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8752fdd9b63b71bc25e32cd40c4a68cd', 'text': 'Figure 8-24 IoT Device FQDN Attribute Being Modified', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 602, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '088129f7fa3f8ec24fac0d98c7618e0a', 'text': 'In step 2 of the threat, the FQDN attribute is modified by the attacker exploiting the vulnerability in the public cloud–deployed configuration management virtual instance.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 602, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1ae833f1738ba0ac52d0372bcea692f9', 'text': 'Figure 8-25 illustrates the redirection of the devices to the malicious command and control center.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 602, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '8c28d6c5bfebd3012fc3ee09bf0662c7', 'text': "Malicious domain (C&C) 5GMEC CM, PM, FM for Applications%%'OTdeVices SP Applications & Data Network ¥a [ ——— [ 4 [ ———— G = 'J'.O ((A)) 4—?\_4—\* = gNB - L 5G MEC Centralized 5G Core uw", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 603, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '138b8829036ad8abb350c6739adf7cac', 'text': 'Figure 8-25 IoT Devices Being Redirected to the C&C Server', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 603, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4c09ccbb5b16f336346f808f6ea0455d', 'text': 'In step 3 of the threat, the IoT devices now reach out to the malicious domain instead of the CM/PM/FM domain of the device vendor. The malicious domain could also be C&C, which now will take control of all the devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 603, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e4836a5b31e8bf73970e43ad6a5d55ef', 'text': 'Figure 8-26 illustrates an example of how the malicious C&C center takes over the IoT devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 603, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '843958063dbf05ec55930e9b0289a4d7', 'text': "ﬁ ' ) Malicious domain (C&C) 5GMEC CM, PM, FM Applucatlons%%mdewces i;‘i' SP Applications & Data Network fa R w e e | IJ.. = g ( A) ‘\_’E‘—'\_ 1 g\\B Centralized 5G Core 56 MEC", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 604, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'afbe83ded2b88f942b45302e63229d34', 'text': 'Figure 8-26 IoT Device Being Exploited by the C&C Server', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 604, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '34b1560c762309778de31fcb68a3e678', 'text': 'The C&C node will now start pushing rogue updates with malicious code in it. The primary intention of the attacker is to understand the behavior of the system (for example, what’s the busy hour of the network, what kind of data is being transmitted and received, and so on).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 604, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7c993c5c9a3ed20b03a0fdf26a23b261', 'text': 'Figure 8-27 illustrates how IoT devices start a DDoS attack toward the 5G infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 604, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '53d73b229dbcc626e8976131c830beb6', 'text': '—dB Malicious domain (C&C) 5G MEC CM, PM, FM for [oT devices Apphcatlons%% SP Applications & Data Network PSR ——— e | [P ——— PR ) e T e [t z JO. g\\B 5G MEC Centralized 5G Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 605, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0aa9066bdad8215a725c594b69606386', 'text': 'Figure 8-27 IoT Devices Causing DDoS Attack Toward the 5G Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 605, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'af1b893542d7a85bdf7d92bb299d77ae', 'text': 'Once the attacker has enough of the devices under control, the devices can now be used to launch attacks on the service provider’s network or any other network. Once the network infrastructure is compromised via DDoS, the attacker can launch signaling or paging attacks, which could overload the control plane of the service provider.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 605, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '161bc100c14201e866f8d72c17e7070b', 'text': 'Mitigation Example', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 605, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'efe35458a3143cd51014e1fd048201b3', 'text': 'Some of the key methods to mitigate the device-based threats are the secure DNS solutions (DNSSEC, DoH, and Secure DNS) unless the device does not', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 605, 'parent\_id': '161bc100c14201e866f8d72c17e7070b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d488d87f7d9247f3faae06250ffa833', 'text': 'use DNS at all. A majority of service providers today are planning to deploy devices that use ZTP with the provisioning based on the cloud platform.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 606, 'parent\_id': '161bc100c14201e866f8d72c17e7070b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '93e7efad2a9bf420466b7ed7ca55e6df', 'text': 'The mitigation technique illustrated in Figure 8-28 is that of the Secure DNS solution, which resolves the DNS query from the IoT device. If the FQDN is changed maliciously to a C&C domain, the secure DNS solution would block the domain and not allow the device to be connected to it.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 606, 'parent\_id': '161bc100c14201e866f8d72c17e7070b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'eb2b41fa3cafc966f6abc72e24a40d0a', 'text': 'Malicious domain blocked DIA (Direct Intermet Access) loT devices A Malcious domain (C&C) Secure DNS faye AN loT devices exiting hia internet using N6 Secure ONS server [P interface / Gi interface config as part of the loT slice config / PCF policy SP Applications & Ve Data Network on the UPF w o= J IOO ——me— B L Centralized 5G Core [ -] 5G MEC w L', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 606, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '623e73c96026634fd8e8db164f4d94a9', 'text': 'Figure 8-28 Securing DNS Layer to Mitigate the Attack Scenario', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 606, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '783870ca05c466face2335cd99f2f0b1', 'text': 'The advantage of the Secure DNS solution is that there is no dependency on the type of device or operating system. The only configuration the service provider has to perform is to use the Secure DNS solution IP address as the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 606, 'parent\_id': '623e73c96026634fd8e8db164f4d94a9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '871db064f4e3dd2a34583189bd5efd94', 'text': 'DNS IP address in the FQDN attribute template being pushed from the provisioning or configuration management toward the devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 607, 'parent\_id': '623e73c96026634fd8e8db164f4d94a9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '56ded8923b37d666d2634b52d9f13e9d', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 607, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fc6371a1db7697b225c02fba0c45accd', 'text': 'There needs to be multiple security layers to ensure mitigation of device-based threats. The threat surfaces and the security capabilities might vary by deployment. Depending on the sophistication of the attack and the network deployment method followed by the service provider, no single type of mitigation technique will be fully effective, as can be seen in the Figure 8-29.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 607, 'parent\_id': '56ded8923b37d666d2634b52d9f13e9d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '28b6d372a303cae9e311d2d32049a48d', 'text': "+ Secure on-prem hosted ZTP and provisioning servers + Secure AP! interface from the 5GC to + Secure air interface using the 3¢ party loT servers + Secure against inbound DDoS atfacks encryption .\_\_\_ + Ensure isolation between loT slice and other slices by using DDoS protection g+ Secure AP! from the loT Application + Ensure the traffic s inspected and servertothe loT Core components segmentation along with Anti-malware is applied to prevent malware to spread within the network (R e ((A)) —E— [ 4 = MEC/ Centralized DC SPloT Applications & Internet l 0 Secure cloud hosted ZTP and provisioning servers \* Inbuit Hardening (Hardware and + Secure backhaul using encryption and 0 authentication using mechanisms such Secure loT application servers to prevent data Software) 2 IPsec using SecGW exilration + Secure devices by using identfication, ' Secure CMIPMIFM layers authentication, access and certfication + Secure backhaul against DDoS attacks 0 by using DDoS profection Enhanced monitoring of loT devices using remote management monitoring solutions + Secure DNS interactions to / from the device", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 607, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b75cdd81bb8ac91f4a0b93f8fb30fa18', 'text': 'Figure 8-29 Multiple Layers of Security Required to Mitigate IoT Threats in the Given Scenario', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 608, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ee8a4cded303412b6ef0f5eaa5af619', 'text': 'When you’re planning for consumer IoT deployments, which is very cost- sensitive, care should be taken to ensure multiple layers of isolation, device monitoring, and granular access control are applied. Figure 8-30 provides the summary of all the multiple security layers required to secure the network from device-based threats. Depending on the network infrastructure of the service provider that needs to be secured from the devices, and the type of devices catered for by the network, one or multiple security layers could be chosen from those highlighted in the figure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 608, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '970a87d77b32e9219db4b7351fdeb8c0', 'text': '5G MEC Applications CM, PM, FM for l—’ %% loT devices SP Applications & Data Network Fa | 7 [ w [ IJ.. ((A)) 4—»\_‘—’\_ Centralized 5G Core 5G MEC 1.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 609, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '70f004bb9dc921baf8788cfe48da99d0', 'text': 'L) L UE', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 609, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a44aed5d23f77c0d023c436ea3dc2e4e', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 609, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e765f5b8028109ad458c7f323699879b', 'text': 'Figure 8-30 Multilayered Security for Securing IoT Devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 609, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3eb4c637b79cc96a41b0212820c4315a', 'text': 'Key Acronyms', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 609, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '595c3e128c45b81aa223d8137449d46f', 'text': 'Acronym Expansion 5GC 5G Core AAA Authentication, authorization, and accounting AMF Access and Mobility Management Function AUSF Authentication Server Function C-V2X Cellular [nd] vehicle-to-everything C&C Command and control C2C Command and control CNF Cloud-Native Function COBOT Collaborative robots CSC Communication services consumer CSp Communication services provider DDoS Distributed denial of service DMZ Demilitarized zone DNS Domain Name System DoS Denial of service', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Acronym</th><th>Expansion</th></tr></thead><tbody><tr><td>5GC</td><td>5G Core</td></tr><tr><td>AAA</td><td>Authentication, authorization, and accounting</td></tr><tr><td>AMF</td><td>Access and Mobility Management Function</td></tr><tr><td>AUSF</td><td>Authentication Server Function</td></tr><tr><td>C-V2X</td><td>Cellular [nd] vehicle-to-everything</td></tr><tr><td>C&amp;C</td><td>Command and control</td></tr><tr><td>C2C</td><td>Command and control</td></tr><tr><td>CNF</td><td>Cloud-Native Function</td></tr><tr><td>COBOT</td><td>Collaborative robots</td></tr><tr><td>CSC</td><td>Communication services consumer</td></tr><tr><td>CSp</td><td>Communication services provider</td></tr><tr><td>DDoS</td><td>Distributed denial of service</td></tr><tr><td>DMZ</td><td>Demilitarized zone</td></tr><tr><td>DNS</td><td>Domain Name System</td></tr><tr><td>DoS</td><td>Denial of service</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 610, 'parent\_id': '3eb4c637b79cc96a41b0212820c4315a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'f6faa1b07cfb7a6c338077dd2e197be2', 'text': 'DSRC Dedicated short-range communications eMBB Mobile broadband FQDN Fully qualified domain name IAM Identity and Access Management IoT Industrial Internet of Things IoT Internet of Things M2M Machine-to-machine MEC Multi-access edge compute MFA Multiple factor authentication mloT Massive Internet of Things MQTT Message Queuing Telemetry Transport NAC Network Access Control NF Network Function NPN Non-public network NSaaS Network slice as a service OBU On-board unit oT Operational technology PCF Policy and Charging Function PNI-NPN Public Network Integrated NPN', 'metadata': {'text\_as\_html': '<table><thead><tr><th>DSRC</th><th>Dedicated short-range communications</th></tr></thead><tbody><tr><td>eMBB</td><td>Mobile broadband</td></tr><tr><td>FQDN</td><td>Fully qualified domain name</td></tr><tr><td>IAM</td><td>Identity and Access Management</td></tr><tr><td>IloT</td><td>Industrial Internet of Things</td></tr><tr><td>IoT</td><td>Internet of Things</td></tr><tr><td>M2M</td><td>Machine-to-machine</td></tr><tr><td>MEC</td><td>Multi-access edge compute</td></tr><tr><td>MFA</td><td>Multiple factor authentication</td></tr><tr><td>mloT</td><td>Massive Internet of Things</td></tr><tr><td>MQTT</td><td>Message Queuing Telemetry Transport</td></tr><tr><td>NAC</td><td>Network Access Control</td></tr><tr><td>NF</td><td>Network Function</td></tr><tr><td>NPN</td><td>Non-public network</td></tr><tr><td>NSaa$</td><td>Network slice as a service</td></tr><tr><td>OBU</td><td>On-board unit</td></tr><tr><td>oT</td><td>Operational technology</td></tr><tr><td>PCF</td><td>Policy and Charging Function</td></tr><tr><td>PNI-NPN</td><td>Public Network Integrated NPN</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 611, 'parent\_id': '3eb4c637b79cc96a41b0212820c4315a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'd719cf1a1442329c49df7f734bff4163', 'text': 'RAT Radio access technology RBAC Role-based access control SBA Service-based architecture SBI Service-based interface SDN Software-defined network SMF Session Management Function SNPN Standalone NPN SSL Secure Sockets Layer TCG Trusted Computing Group TEE Trusted Execution Environment TLS Transport Layer Security TPM Trusted Platform Module UDM Unified Data Management UE User equipment uIcC Universal integrated circuit card UPF User Plane Function V2X Vehicle-to-everything VNF Virtual Network Function AN Zero-Touch Security', 'metadata': {'text\_as\_html': '<table><thead><tr><th>RAT</th><th>Radio access technology</th></tr></thead><tbody><tr><td>RBAC</td><td>Role-based access control</td></tr><tr><td>SBA</td><td>Service-based architecture</td></tr><tr><td>SBI</td><td>Service-based interface</td></tr><tr><td>SDN</td><td>Software-defined network</td></tr><tr><td>SMF</td><td>Session Management Function</td></tr><tr><td>SNPN</td><td>Standalone NPN</td></tr><tr><td>SSL</td><td>Secure Sockets Layer</td></tr><tr><td>TCG</td><td>Trusted Computing Group</td></tr><tr><td>TEE</td><td>Trusted Execution Environment</td></tr><tr><td>TLS</td><td>Transport Layer Security</td></tr><tr><td>TPM</td><td>Trusted Platform Module</td></tr><tr><td>UDM</td><td>Unified Data Management</td></tr><tr><td>UE</td><td>User equipment</td></tr><tr><td>uIcC</td><td>Universal integrated circuit card</td></tr><tr><td>UPF</td><td>User Plane Function</td></tr><tr><td>V2X</td><td>Vehicle-to-everything</td></tr><tr><td>VNF</td><td>Virtual Network Function</td></tr><tr><td>VAN</td><td>Zero-Touch Security</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 612, 'parent\_id': '3eb4c637b79cc96a41b0212820c4315a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd262ef9a25acc14e50adc593d08b9860', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 612, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '20bd86a8f90d59d91df057c0b78297ba', 'text': '“Cisco Annual Internet Report (2018-2023) White Paper,” https://www.cisco.com/c/en/us/solutions/collateral/executive- perspectives/annual-internet-report/white-paper-c11-741490.html Pramod Nair, “Securing Your 5G–Infrastructure to the–Edge and Beyond,” Cisco Live, Cisco Public, March 30, 2021', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 612, 'parent\_id': 'd262ef9a25acc14e50adc593d08b9860', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f15ad9adc5cf1ce0cee9e7f4336982d5', 'text': 'Pramod Nair, “Securing Your 5G Network End to End,” Cisco Live APJC, Cisco Public, April 30, 2019', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 613, 'parent\_id': 'd262ef9a25acc14e50adc593d08b9860', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7fcb90c86da5f853430b4f3402eb5519', 'text': 'Michael Geller and Pramod Nair, “Cisco 5G Security Innovation with Cisco,”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 613, 'parent\_id': 'd262ef9a25acc14e50adc593d08b9860', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5363f6bf924c2189157476f0bdc21e17', 'text': 'https://www.cisco.com/c/dam/en/us/products/collateral/security/5g- security-innov-wp.pdf', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 613, 'parent\_id': 'd262ef9a25acc14e50adc593d08b9860', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5c0213382fbdb4c3c9e2e62942be7260', 'text': '“Examining the Security of Wi-Fi 6 and 5G White Paper,” https://www.cisco.com/c/en/us/solutions/collateral/executive- perspectives/white-paper-c11-743921.html', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 613, 'parent\_id': 'd262ef9a25acc14e50adc593d08b9860', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b8182a9e3f8a6ad4fa766449a6058e81', 'text': '“What is Trust?” Cisco Public,', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 613, 'parent\_id': 'd262ef9a25acc14e50adc593d08b9860', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ab5ee0cda3b68b1f6992de31d2fab30', 'text': 'https://www.cisco.com/c/en/us/solutions/service-provider/5g-what-is- trust.html', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 613, 'parent\_id': 'd262ef9a25acc14e50adc593d08b9860', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '011367de9751e3f23b7764ed389c3a73', 'text': 'Robbie Grue, “DoH! What’s all the fuss over DNS over HTTPS?”, Cisco Public, https://umbrella.cisco.com/blog/doh-whats-all-the-fuss- about-dns-over-https', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 613, 'parent\_id': 'd262ef9a25acc14e50adc593d08b9860', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5e452b8906087ff4a56f2a0815f1dbbd', 'text': '“Trusted Platform Module (TPM) Summary,”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 613, 'parent\_id': 'd262ef9a25acc14e50adc593d08b9860', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '070a9d3f006694062373fdc0d489a469', 'text': 'https://trustedcomputinggroup.org/wp-content/uploads/Trusted- Platform-Module-Summary\_04292008.pdf', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 613, 'parent\_id': 'd262ef9a25acc14e50adc593d08b9860', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '616c78d877153ecde07eab242a21388d', 'text': '3GPP TS 29.561 V17.1.0: Interworking Between 5G Network and External Data Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 613, 'parent\_id': 'd262ef9a25acc14e50adc593d08b9860', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a54d72f632843d5360acd53018f946b7', 'text': '3GPP TS 28.807 V17.0: Study on Management of Non-Public Networks (NPNs)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 613, 'parent\_id': 'd262ef9a25acc14e50adc593d08b9860', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '6832591d447c3879959a109f0f6ecd95', 'text': 'Chapter 9. Securing 5G Use Cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7584de3cdef42174f2c66a242b9f115a', 'text': 'After reading this chapter, you should have a better understanding of the following topics:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4191c15f1a2b8ba4cd047592620e541c', 'text': '• Key 5G use cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '69c139bb189e628797ec1c05ae7dc811', 'text': '• Key threat surfaces in different 5G use cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '13b14981a53f52d0343844b41ede4ced', 'text': '• Key security controls for securing 5G use cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7344e8adac609581a41d2c9e4acb1f7f', 'text': 'This chapter will take you through the different 5G IoT use cases, their respective threat surfaces, and mechanisms to mitigate the threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '92b2e0ae1fe28b73b387e1f3d427c950', 'text': 'This chapter will be of particular interest to the following members of teams from enterprise 5G consumers, 5G service providers, and cybersecurity vendors planning to provide security layers for 5G:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e9b9bc8ff2b0d778213a0a638aa71d2c', 'text': '• Strategy teams of service provider and enterprise verticals looking at 5G use cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '34d0f8ea6454d31cc85756898cd76a55', 'text': '• Security strategy teams within service provider and enterprise verticals deploying 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0d1d89d78c38fd10290f432ebac20fbf', 'text': '• Cloud computing and data center teams involved with 5G strategy and deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0f03388c95932529f28ba08d8865ee97', 'text': '• Security architects and design teams looking at securing the mobile infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9fd121d0792f292815629213223864e0', 'text': "• Enterprise solution and security architects deploying standalone private/NPN 5G or utilizing a service provider's 5G slice network", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '95101efe01080ae2be9ca861712158a9', 'text': '• Government departments deploying 5G for smart city projects', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a5264e2a92cc79c18738030e4bc43674', 'text': '• Cybersecurity vendor teams looking to secure 5G use cases for their customers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e86e44be51439e68b032b630acddee52', 'text': '• Product managers of cybersecurity vendors', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '23782ea984246a6bd675782ddcb15b9e', 'text': 'This chapter focuses on 5G use cases that can have a mixture of different deployment methods, such as standalone private 5G/non-public network (NPN), public 5G, and hybrid 5G deployments with integrations between the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 614, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3ca2119a9a9595c6f1c4aeeeb23db26a', 'text': 'enterprise-deployed NPN and the service provider network. The hybrid 5G deployment is also called a public network infrastructure (PNI) NPN.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 615, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f993319a23451fd316288add80fe0d26', 'text': "The industrial IoT (IIoT) use cases discussed in this chapter make use of enhanced mobile broadband (eMBB), machine-to-machine (M2M), and massive Internet of Things (mIoT) domains. Although Chapter 8, “Securing Massive IoT Deployments in 5G” is dedicated to mIoT/consumer IoT, some of the use cases in this chapter would cater for mIoT devices. Although the use cases mentioned in this chapter are yet to be fully realized, there are engagements that I am working on with service providers that made me realize that the key use cases require a broader set of security controls. The main reason being that any use case that will be deployed using 5G will need to cater for legacy and existing network infrastructures and devices in the network. This chapter is a sincere attempt to spread the message of the impending threat surfaces I've encountered during my discussions with customers and the mitigation mechanisms that need to be undertaken to enhance the security of the network.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 615, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed4dd6046da40731b2b34b4729a28cdf', 'text': 'Other use cases, such as securing smart cities, will include all the use cases discussed in this chapter. There are various industry frameworks, standardizations, and open source communities working toward achieving a secure smart city concept, and its realization is still quite a few years away. There are many more use cases, some selected for further study for 3GPP Release 18, which is expected to be released around December 2023.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 615, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f086a91ec5470d4129b8a9bf21ae5889', 'text': 'With the aim of keeping the chapter as close to a real scenario as possible, this chapter includes the following topics, which has traction in the market today:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 615, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '88eafc45c379ced1e7eb294870bde87d', 'text': '• Secure 5G smart factory and manufacturing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 615, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a1bf7f3434ba447a2c485d7565a2b0e', 'text': '• Secure critical infrastructure (example considered for secure 5G energy utility deployments)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 615, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a9c67135bb84e877c245ae77d7362a9', 'text': '• Secure 5G-V2X', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 615, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '643d6d030ea9e9ab522650f7cc36e0e1', 'text': 'The example of secure energy utility could be applied to other critical utilities with variations in the use case, such as securing water utilities. As discussed in Chapter 8, the IoT/IIoT devices being used in the 5G deployments to fulfill the use cases might be smart or not-so-smart devices. These devices will have varying levels of intelligence and security awareness and therefore require different levels of security controls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 615, 'parent\_id': '6832591d447c3879959a109f0f6ecd95', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'bf3ba028ffa4f9e419cd8672cc171761', 'text': 'Secure 5G Smart Factory and Manufacturing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 616, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c37158f0169dcb13ded48bf039db928c', 'text': '5G technology is touted as the key enabler of Industry 4.0. This is due to the advantages that 5G provides, such as higher throughput, lower latency, flexibility in deploying the 5G components in the cloud or on the premises, openness in integration with applications made by third-party developers, and the flexibility in deploying the 5G infrastructure. With sensors that are deployed in factories, machines will benefit from this fast and reliable low- latency data transfer. Driverless transport systems within the manufacturing factory will benefit from the low-latency features of 5G. The 5G technology is still young and evolving. Companies are starting to market various products and services that will run on 5G. This transformation will be a multiyear journey, as production deployments require stable specifications, production- quality implementations, and supportive ecosystems to be in place before widespread availability.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 616, 'parent\_id': 'bf3ba028ffa4f9e419cd8672cc171761', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1cb8221583e56db983eca379f78b0c3d', 'text': 'One of the key enablers of improved efficiency in the manufacturing industry is the use of robotics. Automated manufacturing solutions using robotics improve efficiency and safety, automate repetitive tasks, reduce margins of error, and enable human workers to focus on more productive areas of the operation. Fully autonomous robots in manufacturing are commonly needed for high-volume, repetitive processes. Other manufacturing automation solutions include robots performing heavy tasks such as lifting, holding, and moving heavy pieces. The robots in the factory are in continuous production and movement, which requires near real-time implementation of commands.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 616, 'parent\_id': 'bf3ba028ffa4f9e419cd8672cc171761', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4f3f5937a67a29fcc6f199978920970d', 'text': 'Manufacturing factories also have sensors deployed all over for various reasons, such as collecting data from disparate devices and systems to enable different machines to talk to one another. This creates seamless connectivity throughout the factory for equipment monitoring, data collection from different systems to predict any equipment failure, and triggering protocols related to site and equipment maintenance.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 616, 'parent\_id': 'bf3ba028ffa4f9e419cd8672cc171761', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd8c7527d3246359f02179a86d9560e1e', 'text': 'Figure 9-1 shows one of the possible different methods of deploying 5G to cater for a manufacturing use case.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 616, 'parent\_id': 'bf3ba028ffa4f9e419cd8672cc171761', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '55273b61f6e72f08463dfc8e2b7514ba', 'text': '[P S ——— = Public Cloud & Internet - T IT Network s ] - 5G-lloT | d & Network d [o— I o — .Q. g\\B =B & § == 5GC MEC DC [ Y [ Smart Factory', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 617, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '816b40814258a1fb6ddd0f472f8f8e6f', 'text': 'Figure 9-1 Example of a 5G Smart Factory Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 617, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4d056235692cb46d44c664f3c916d07d', 'text': "As shown in the Figure 9-1, the manufacturing entity, such as a smart factory, can be realized by using the service provider's 5G network coverage. The 5G coverage could be provided by Fixed Wireless Access (FWA), an open RAN deployment model where Distributed Unit (DU) and Centralized Unit (CU) or a micro/pico cell could be deployed at the factory premises. The service provider would then allocate a network slice and configure the required quality of service (QoS). The QoS would ensure that the required availability and other SLAs are met to provide the required service to the smart factory/manufacturing use case. This scenario could also be fulfilled by using the network slice as a service (NSaaS) method, where the manufacturing/smart factory entity is the communications service customer (CSC) and the service provider with the 5G network components is the communications service provider (CSP). The CSC will be provided access to the management of the", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 617, 'parent\_id': '816b40814258a1fb6ddd0f472f8f8e6f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7093f747a5160fc505385dab4f4a6f16', 'text': 'service layer of the network slice provided by the CSP. A privileged user such as an admin from the CSC can then configure the required QoS for the 5G NFs within the network slice catering for the manufacturing/smart factory facility. Figure 9-2 illustrates the different IIoT devices and the IIoT network within the 5G smart factory considered in this example.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 618, 'parent\_id': '816b40814258a1fb6ddd0f472f8f8e6f', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '17d7b1c2e03cac79c29d27cb344aa5b2', 'text': 'Manufacturing Sensors Robots loT Applications & OT Network Internet SRS Rep— o] d (y) le —HE—E— B = SP Applications & ONB MEC DC 5GC [nternet - i ; [y (e 4 Smart Factory 5G Network Automated Galeway lloT Application Transport Server', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 618, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9f98a05f5958e5c4c9cb697506badce5', 'text': 'Figure 9-2 Components of the 5G Smart Factory', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 618, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b2d8013095707fe70591d5a3d6827f56', 'text': 'Figure 9-3 shows another option of 5G deployment by using private 5G or non- public network (NPN) to cater for 5G smart factory and manufacturing use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 618, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '1ac05a18cf9846fcb7189b67de0ca046', 'text': '- ] [T Network ) C ? Public Cloud & Internet - MEC applications for smart factory devices (y) \_ gNB E o T’ ~ LI &2 E 8] A = ENTD 5GC —\_ ﬁﬂ Network E gN\\B T cmmmm—— Manufacturing Plant Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 619, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e6aa0e5af88d33232a34ed70a43764e', 'text': 'Figure 9-3 PNI Non-Public 5G/PNI Private 5G Deployment Example', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 619, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fb28260e03f6a6bebc797b83339508ab', 'text': "In the deployment method shown in Figure 9-3, 5G radio nodes (gNB/CU/DU) and the key user plane components are deployed on the premises of the smart manufacturing facility, and the 5G control plane is deployed on the service provider's premises. These deployments are called public network integrated private 5G network/non-public network (PNI-NPN). This method of deployment is considered when ultra-reliable low-latency communications (URLLC) needs to be deployed. As URLLC is extremely latency sensitive, deploying the non-3GPP NFs, such as applications catering to the smart factory use cases, and 3GPP NFs, such as User Plane Functions (UPFs), closer to the URLLC devices would help you meet the stringent latency requirements. In such deployments, the enterprise/smart factory would retain complete control over the flow of 5G traffic, including the 5G air interface (Uu) communications", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 619, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f8ac696df7dc82af702a6e41ed625b0e', 'text': 'between the 5G IIoT device/5G network gateway and the 5G access node (gNB) components. If all the components, including RAN, 5GC user plane, and control plane, are deployed and catered for by the enterprise, it is referred to as a standalone private 5G/NPN network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 620, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e7e230d953b79409969bff0a1984f79', 'text': "Another deployment method, shown in Figure 9-4, has the entire 5G radio and 5G Core user and control plane components deployed on the premises of the smart manufacturing facility, and there is no dependency on the service provider's premises. These deployments are called standalone private 5G networks/non-public networks (SNPNs). These deployments will be used by industry verticals and enterprises that need the 5G use cases deployed and executed within their premises. At the time of writing this book, national security government organizations and smart factory industry verticals were undergoing initial standalone non-public 5G network deployments.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 620, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'b8f04e57f584e93c8325fadb4c212722', 'text': "] Public Cloud & Internet [ I ——————— [T Network :-'-E ; - [loT Network MEC applications for d (y) smart factory devices N O gNB AL o= ‘i 1 5GC X (A ENTDC e g\\B YR —— [ ————— 4 Manufacturing Factory Network", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 621, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c89c4d76ce4029b7722c276a70d1957a', 'text': 'Figure 9-4 Standalone Private 5G/Non-Public (SNPN) 5G Deployment Example', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 621, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1605667f3d1326d863d3058944ffca51', 'text': 'Threats in 5G Smart Factory Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 621, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '232a4a867b5714fc7d6cdd0d7436d2a0', 'text': "5G introduces the technology advancement required to fulfill URLLC use cases in the smart factory and manufacturing sector, thereby improving productivity. 5G's enhanced deployment methods, such as multi-access edge computing (MEC), allow robots and collaborative robots (cobots) to be monitored and updated in near real time as the environment changes. Where, for example, customizations to specific products are needed, 5G IoT can be used to feed precise requirements for each product through to the robot or cobot to create personalized products and facilitate integration with third-party ecosystems using APIs. This openness in technology, however, also introduces an expanded threat surface, as illustrated in Figure 9-5 and described in the list that follows:", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 622, 'parent\_id': '1605667f3d1326d863d3058944ffca51', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f28428b4b63acaa8c3754eabe6346b29', 'text': 'CM, PM, FM layer attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 623, 'parent\_id': '1605667f3d1326d863d3058944ffca51', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '4d879e94f709850d978cbac6db7af389', 'text': '+ CM, PM, FM layer attack + Exploit lloT MEC Appln + Data exfiltration + API exploitation \* Improper Slice configuration R - - - - % Public Cloud & Internet =7 - - d 5G - lloT Network d ilifi L g\\B MEC DC 5GC 2 b Threats from [T network migrating to lloT network Data exfiltration & Data hoarding DDoS Attack + Malware execution attacks \* |oT firmware attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 623, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '59e6e5c248ce093a5f072c37b9471d8b', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 623, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cb0acded38270b873c5ab91631f3fa61', 'text': 'Exploit lloT MEC Appln', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 623, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '996615848137d033106cc61991d499da', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 623, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5156de1229f6d1b8fd6dfd9703428286', 'text': 'Data exfiltration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 623, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '8e8c036cad7225a3b096c7a4269a34db', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 623, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'UncategorizedText', 'element\_id': '16d292ebf85beb88b58b22c43be86654', 'text': '+', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 623, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '541e63327b9d72efde12d334d834c082', 'text': 'Malware execution attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 623, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'ListItem', 'element\_id': 'e9ce93cb6767ca763243b0cf4c70edac', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 623, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b7e286680b03c4054dae363059f139db', 'text': '|oT firmware attack', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 623, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ca370a5577212ace2e207fa652496ba5', 'text': 'Figure 9-5 Key Threats 5G Smart Factory and Manufacturing Use Case', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 623, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '61506972d471a6df951e03e454f83a73', 'text': "• One of the key risks in today's manufacturing network that is also important in the 5G–smart factory/manufacturing use case is the migration", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 623, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0168cc6cf984d272cbf8892534148d01', 'text': 'of threats from the IT network to the IIoT network. The employees and guests in the IT enterprise network of the factory are susceptible to malware and other risks due to phishing and other such attacks on the users of the IT network, as shown in the Figure 9-6. Although this is not a pure 5G threat surface, if this risk is not mitigated or the security control planned in the design, it will impact the 5G–IIoT network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 624, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '0904837d744b553f6d8eb00f69429b3c', 'text': '0 0 Attacker [T Network ] :-5..! — -+~ Public Cloud & Internet ES Malware -- migrating from IT network to 5G- [loT network 5G-lloT \_ ) Network d Iﬁi. ~ T’ =] =] gNB ~ 5 == MEC DC 5GC 0', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 624, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '90a11210ba517fe943ff5836d0f110c0', 'text': 'Figure 9-6 Example of a Threat Surface from an IT Infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 624, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c3ee8d006ec2cd154a7e35d5672a5408', 'text': '• The attacker uses the Internet-facing server in the IT network of the factory to launch an attack into the 5G–IIoT network due to improper isolation. Once the cobots and 5G–IIoT devices are under the control of', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 624, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '20b1fa7adf8550e00834ef9cb8225cfb', 'text': 'the attacker, the attacker could launch a DDoS attack on your 5G infrastructure or conduct data exfiltration.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 625, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da2a4683c7deed5915c276b90300f581', 'text': '• With regard to application-based threat surfaces, non-3GPP 5G NFs and 5G–IIoT devices are susceptible to patches or updates with embedded malicious code, as shown in Figure 9-7. This is basically done at a couple of levels. One of the primary insertion points of malicious code is the update server of the 5G–IIoT device and application vendor itself. The other key risk area for malicious insertion of code is the management network/operational technology (OT) network of the smart factory. Due to the implementation of weak authentication and authorization in the management layer of the 5G–IIoT network, the attacker could launch a privilege escalation attack on your network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 625, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '633d461bb6bff762e7e3b09f02c1bf49', 'text': '9 A Attacker includes malicious code in Attacker the patch update for the 5G-IloT devices / applications ’ [T Network 7] :-:-E ? Publ Cloud & Internet C 4 5G-lloT \_ Network ~ 71 gNB % i = MEC DC () 5GC 6 . Forced Malware update on the 5G-IloT devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 626, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8f9edd65995219c864ac32978d3261bb', 'text': 'Forced Malware update on the 5G-IloT devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 626, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '64d5fa738aed1cd1e150f8a9d5a5afda', 'text': 'Figure 9-7 Embedded Malicious Code in Firmware and Application Updates', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 626, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9372a078c23c873d3f7d2913d6c58db5', 'text': 'Updates', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 626, 'parent\_id': '64d5fa738aed1cd1e150f8a9d5a5afda', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '90927334c11f0ba996d30d7b5a3aaa11', 'text': '• API is another area that has an increased risk factor in 5G smart factory deployments. 5G brings in service-based architecture (SBA), which uses API-based communication both internally to the 3GPP 5G NFs and in', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 626, 'parent\_id': '64d5fa738aed1cd1e150f8a9d5a5afda', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '212203e78ade2780174ecd02bda792fd', 'text': 'interactions with non-3GPP NFs using the Network Exposure Function. API will also be the preferred mode of communication between the 5G– IIoT devices and the corresponding management layer. Although 3GPP has recommended the Common API Function (CAPIF), the security feature implementation of the API, such as granular authentication and authorization, is up to the developer. Weak API implementation, such as passing too much information in error messages, will lead to exposing the type and version of the web server to the attackers, which could then be exploited to launch a targeted attack on the API web server. Attackers have to gain access to only a few accounts, or just one admin account, to compromise the system, which could lead to the leakage of legally protected, highly proprietary, sensitive information in your smart factory network. Insecure communication links between the headquarters (HQ) and the multiple 5G smart factory sites are susceptible to man-in-the- middle (MitM) attacks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 627, 'parent\_id': '64d5fa738aed1cd1e150f8a9d5a5afda', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd0a21a7b0e8a2af1e48e217273ceba59', 'text': 'Securing the 5G Smart Factory', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 627, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '28fc328fbb86b86d7c89bb4752414a64', 'text': '5G technology will enable manufacturers deploying IoT technologies to migrate to Industry 4.0, optimize production, and build new generations of products and services. This deeper integration between 5G, IT, cloud, and industrial networks requires cybersecurity capabilities that can protect your production environment and assets as well as maintain operations. Service providers deploying technology enablers, such as MEC and network slicing, to implement smart factories or manufacturing should deploy security controls to protect their infrastructure from risks such as DDoS attacks, data hoarding, and data exfiltration.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 627, 'parent\_id': 'd0a21a7b0e8a2af1e48e217273ceba59', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '748433e60bf8dc5c2a290f57915f32ef', 'text': 'Securing the 5G smart factory and manufacturing entities will require a secure process and multilayered security controls. The secure process should include following IIoT security-related standards such as the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 627, 'parent\_id': 'd0a21a7b0e8a2af1e48e217273ceba59', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c068f6dc21a07ccb28e42c621dcf4d48', 'text': '• Segmentation and isolation: 5G smart factory deployment design should consider an industrial demilitarized zone (DMZ) with separate firewall instances or appliances for data traffic between the enterprise/IT network and the wider factory IIoT network and jump servers/jump host server for managing and accessing the IIoT devices from the IT network, if required, as shown in Figure 9-8. The separate firewall/gateway for the IT and IIoT networks will provide hardware-enforced isolation, preventing arbitrary connections to act as attack vectors from the Internet toward the IIoT', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 627, 'parent\_id': 'd0a21a7b0e8a2af1e48e217273ceba59', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a1d1414089c9036d1050e6eecb02d63', 'text': 'network. Separate protection should be provided for legacy devices. The network devices should have support for cybersecurity protocols such as access control lists (ACLs), NetFlow, TrustSec, IPsec, and MACsec. A network access controller (NAC) should be dedicated to creating and enforcing network security policies. The NAC solution you choose should provide software-based device-level segmentation to manage network access control at scale. Figure 9-8 illustrates the segmentation and isolation security controls for the 5G smart factory use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 628, 'parent\_id': 'd0a21a7b0e8a2af1e48e217273ceba59', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '9f371a8f9386a84389951940c5285e05', 'text': '= =] [T Network Segmentation & Isolation between [T & 5G - lloT Network - 1 - Firewalls / Gateway pumns g eadunnnnanans Public Cloud & Internet Jumpéerver Mz, &= ceessssassssassasanes d d - ? Standalone . W NPN Deployment option R g\\B a 5GC §G - lloT Smart Factory Network A — ) Service Prowder 5G Network ((A Public Network Integrated g | NPN Deployment N 5G MEC 56C', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 628, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '692e6fa0a6d6838a3ee8bd1fb5244262', 'text': 'Figure 9-8 Segmentation and Isolation Between IT and 5G–IIoT Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 629, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bdeef99b5314d5f8c24af846ece85726', 'text': '• Enhanced visibility and anomaly detection: Deploying security controls for your smart factory 5G–IIoT network can quickly become very complex, especially if your industrial network is dispersed across an entire country or many remote industrial sites. For your security deployment to be successful, the security solution you select must be able to scale easily and at a reasonable cost across your entire organization. To have an effective security strategy, recommended practice dictates selecting IIoT network devices with built-in security sensors that enable you to collect the information required to provide comprehensive visibility, analytics, and threat detection. Having an built-in sensor in your 5G–IIoT network automatically uncovers the smallest details of the production infrastructure, such as vendor references, firmware and hardware versions, serial numbers, and so on. The built-in sensor should also identify asset relationships and communication patterns as well as provide you with detailed analysis of inter-device communication and identify any anomaly in behavior, such as unexpected controller modifications or data exfiltration from the 5G–IIoT network to a new host or a new connection to an unexpected host. This will enable you to take action to ensure production continuity and maintain system integrity. The data from the built-in sensors should be consumable by an existing or newly deployed anomaly detection solution, as illustrated in Figure 9-9. The anomaly detection engine (ADE) should be customizable so that you can provide the policy defined for the IIoT devices. This custom policy must be used by the ADE to compare it with the real-time behavior of 5G–IIoT systems; this will ensure that any anomalies in behavior will be detected, thereby immediately improving the time taken to detect. The ADE should also use machine learning (ML) and artificial intelligence (AI) to enhance the efficacy of the threat detection. ML is trained by the security vendors by providing vast amounts of learning data with varying efficiency, depending on the vendor. Recommended practice dictates testing the efficiency of these ML algorithms by creating your own set of learning data and verifying if the ML algorithms actually detect the anomalies. End-to-end visibility on the enterprise IT network and the 5G–IIoT factory network can be provided by utilizing NetFlow telemetry data from the network, creating a baseline of the behavior of network devices, and', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 629, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e3f08e47455b568685e69b516892f2ab', 'text': 'detecting any', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 629, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '04adb47088850466d52cd9261ccc4a69', 'text': 'a', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 629, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '36d0780338d59ce24142e4fb7868cabe', 'text': 'cater', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 629, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6c76863b7d7328d23d4de4a9c011bef5', 'text': 'encrypted packets without the need for decrypting the encrypted traffic. Figure 9-9 illustrates the enhanced visibility security controls for the 5G smart factory use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 630, 'parent\_id': '36d0780338d59ce24142e4fb7868cabe', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '1d2616b0da8f56c8016e9972c47fbd44', 'text': 'Threat Policy defined Al for lloT devices Intel 1R NetFlow, IPFIX, sFlow, NSEL Anomaly Detection Engine - 5G - lloT & OT Network & devices j Lightweight sensor metadata d rafs g = i +— GRAN ; Appllcauon server ! Hypenvisor metadata Container telemetry, Access logs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 630, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dcdb8328eca7e80c6b9da2bcd50d4d1b', 'text': 'Figure 9-9 Anomaly Detection Engine for 5G–IIoT Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 630, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b65957dd058a1fc956b76314b4b6957', 'text': '• API security: For multisite smart factory deployment, the alerts and security events should be sent to the centralized monitoring system in the HQ, which includes the configuration management (CM), fault', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 630, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b3beb0180f5428d85920550b66b80778', 'text': "management (FM) and performance management (PM) for the 5G–IIoT smart factory devices. The CM commands would be configured using the API interface. In NPN deployments, an API mode of communication would be used for any integration between the Network Exposure Function (NEF) and the Application Function (AF). This reasserts the importance of API security, including API connectivity security using Transport Layer Security (TLS), which enhances both privacy and data integrity, as shown in Figure 9-10. Many of the developers building applications do not enforce the right restrictions on what authenticated users are allowed to do. Attackers exploit these flaws to access unauthorized services and perform malicious actions, such as accessing other users' accounts, viewing sensitive files, modifying other users' data, changing access rights, and so on. To mitigate the risks due to improper authentication and authorization, there are a few key steps you could undertake. One of the key steps is to verify if your chosen vendor ships API web servers with default credentials for admin users. The other key method of mitigating weak API implementation is to ensure that the granular authentication can be implemented as shown in Figure 9-10, preventing automated brute-force attacks and credential stuffing attacks, which makes use of lists of known passwords. Figure 9-10 illustrates the API security controls for the 5G smart factory use cases.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 631, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'af1aab779fdc2795d496b865d18c0184', 'text': "Global Policy Engine ' 5G Smart Factory HQ v MFA (CM, PM, FM, for 5G-1loT devices - multiple sites) +|dentity and Access Management P ‘G /TLS Site 1 Site 2 Site 3 5G Smart Factory 5G Smart Factory 5G Smart Factory Network Network Network", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 632, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b12f2dec62e4fb5d1129f9a08bc7c362', 'text': 'Figure 9-10 API-GW Integration with Identity and Access Management', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 632, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e8362b196a6b1df573cc2adb1ac47de6', 'text': 'As Figure 9-10 illustrates, multifactor authentication (MFA) and Identity and Access Management (IAM) should be integrated with a global policy engine that will use a custom policy provided by you as well as input from external sources as input to a trust algorithm to decide access to the resource.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 632, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a2a4b371557eb0a7b7cd74cbf6322cf7', 'text': 'Application-Level Security Controls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 632, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '70957afafc678e6a66dcf92ce9520949', 'text': 'Depending on the 5G deployment opted for by the smart factory, the implementation of the application security controls will vary. If the PNI-NPN method is deployed, as shown in Figure 9-11, the deployment would be based', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 632, 'parent\_id': 'a2a4b371557eb0a7b7cd74cbf6322cf7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '90b84e273ab548ff65c3fce21b17a8f9', 'text': "on a specific slice for the smart factory use case. In the example shown in Figure 9-11, the user plane and some key 5GC NFs, like AMF, SMF, and PCF, will be deployed on the enterprise's premises with SMF integration with a local IAM solution for authentication of users and 5G–IIoT devices.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 633, 'parent\_id': 'a2a4b371557eb0a7b7cd74cbf6322cf7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '3edf5283434b4b2bf259b1dfa2b305cc', 'text': "' Miérosegmentation \* Vulnerabilty Assessment & Forensics lloT MEC ¢ Application ! = [T Network i = s :\\ Public Cloud & Internet -. A g DMz \\ 5G - lloT Smart lloT UPF flo CP lloT MEC ; | NFs rﬂl Factory Network \\ d ( ( ) / Rpplication ) ) — X E an g\\B i == %C 56C Smart Factory Slice Application server", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 633, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7d9d63e368f866f2d346327d66195d5a', 'text': 'Figure 9-11 Securing Applications in the 5G and IIoT Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 633, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '704947283ab0922fda5384a581b094ce', 'text': 'If the enterprise-hosted NPN method is deployed as shown in Figure 9-12, it would be based on a 5G network fully owned and operated by the enterprise. In the example in Figure 9-12, the 5GC components are deployed on the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 633, 'parent\_id': '7d9d63e368f866f2d346327d66195d5a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '266a79adf822639801eaec6a644f7ca5', 'text': "enterprise's premises with integrations with a local IAM solution for authentication of users and 5G–IIoT devices.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 634, 'parent\_id': '7d9d63e368f866f2d346327d66195d5a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '9de88f7adb39cf885dac39c522ac9896', 'text': '\* Application-leve! Policy Enforcement + Microsegmentation + \\ulnerabil Assessment & Forensics Smart Factory 56 Private Network P P F——— UDM UDR API APl AUSF peF Pl 5G - lloT Smart AP d Smart Factory Network Factory | d (A) AMF IAM AL ? § Radius X T i \\( PFCP § == f lloT Appln Application server UPF TN EE— — P — ;', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 634, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '61d157204fbd8aefa54f7945e4ae01e9', 'text': 'Figure 9-12 Securing Applications in a 5G NPN Smart Factory Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 635, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed16a289bbd665c6469ed90617224ae3', 'text': 'The key application controls for the 5G 3GPP and non-3GPP Cloud-Native Functions (CNFs) are based on ensuring proper application dependency mapping, such as applications that are dependent on other applications and services. Any vulnerabilities in the open source software used for building the 5G 3GPP and non-3GPP CNFs should be identified by the solution you select for application security. The solution you choose should enable security teams to implement a secure, zero-trust model for workloads using microsegmentation. This layer of security control must automate the policy generation for microsegmentation using unsupervised machine learning and near-real-time application behavior analysis. It must also normalize these policies based on priority and hierarchy before enforcing the security policies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 635, 'parent\_id': '61d157204fbd8aefa54f7945e4ae01e9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e405a2d7862d71c63a1787b805453b50', 'text': 'Figure 9-13 shows the summary of the security controls for mitigating the threats for the manufacturing use case.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 635, 'parent\_id': '61d157204fbd8aefa54f7945e4ae01e9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'e84776c1f7d1efd5836df83ed830dfd2', 'text': 'T Network — iid Public Cloud & Internet H L - - Mz = [loT CP NFs pnnnnnnnnn, PR——— T 5G- lloT Smart E i T NEC E ? — "Application ~\* Neassssses’ E \'25:1 ‘i Factory Network (( )) — 3 = gNB 2 MEC DC 56C ~k’:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 636, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a6a2c1e783656ef436d03ea6c4249d2c', 'text': 'A wad AR e amma e', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 636, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f6e23c6f15374417ea67c4e648cbcf88', 'text': 'Figure 9-13 Summary of Security Controls to Secure 5G Smart Factory Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 636, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ddbd26c0bbbb24672d24d8ded3057a4a', 'text': 'The aforementioned security controls, along with ongoing standardization efforts on private 5G/NPN 5G deployments, are key for establishing a reliable and secure smart factory and manufacturing solution. Smart factory 5G–IIoT devices such as 5G-enabled robotics and sensors would require integrations', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 636, 'parent\_id': 'f6e23c6f15374417ea67c4e648cbcf88', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2089d208eea9476a267c3e57388e9fa1', 'text': 'with non-3GPP applications at the edge of the network, enabling URLLC use cases for smart manufacturing. A multilayered security control, as shown in Figure 9-13, is necessary to reduce risk and provide a robust security layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 637, 'parent\_id': 'f6e23c6f15374417ea67c4e648cbcf88', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e8496aeb8f0c8a270100cbae0cb9ed21', 'text': 'Critical Infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 637, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '771031df5ed355f7c828c86f5c0fc3a9', 'text': "5G brings advanced connectivity technologies to critical infrastructure providers such as the energy utility sector. 5G can play an essential role in enabling utilities to keep pace with rapid change. There are multiple ways the utility companies, such as energy providers, can make use of the advantages of 5G, such as low latency, network slicing features, and edge deployment modes. Service providers could also monetize the 5G network deployment by reselling parts of the network resources to utility providers. This section will take you through both views—from the energy utility company's perspective and the service provider's perspective.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 637, 'parent\_id': 'e8496aeb8f0c8a270100cbae0cb9ed21', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4e5fbbddf7e33605d89c0728c0f5b96e', 'text': '5G Energy Utility', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 637, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4bd249a7dca6505fb0c2f3c127121472', 'text': "Energy utility companies are seeing demand from their customers to have near- real-time information on usage and pricing. They are also seeing internal demand for real-time identification of faults to reduce the network downtime or outage period. 5G technology with enablers like edge computing deployments for radio and packet core components will help in catering for the aforementioned new requirements from energy utility companies. They also have to cater for some areas of the energy utility company that might have legacy deployments of proprietary control systems, which need to be catered for until the time they are discontinued and taken out of operation, as they will be inefficient and expensive to operate and maintain. Grid operations have expanded over time, leading to a patchwork of legacy control and business environments. Utility operations have recently become a rich target for cyberattacks, given both their national visibility and the expanded attack surface across their increasingly connected assets. Connected assets also carry the risk of physical damage, utility downtime, and breaches of customer data and intellectual property. The energy grid in today's network is vulnerable to the following:", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 637, 'parent\_id': '4e5fbbddf7e33605d89c0728c0f5b96e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ff22323a22da7d943fbb8f91540b5d2d', 'text': '• Lack of compliance with evolving security standards', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 637, 'parent\_id': '4e5fbbddf7e33605d89c0728c0f5b96e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '768031a0994acf676a4a194138ac1207', 'text': '• Legacy nodes and infrastructure elements', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 637, 'parent\_id': '4e5fbbddf7e33605d89c0728c0f5b96e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '26d9cbfc37a4551f225f40ebc2b723b6', 'text': '• Blind spots in the network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 638, 'parent\_id': '4e5fbbddf7e33605d89c0728c0f5b96e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4a67f00c33657c0264d8726ac18770c1', 'text': '• Harsh outdoor environments that affect transmission and delivery', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 638, 'parent\_id': '4e5fbbddf7e33605d89c0728c0f5b96e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '710dac53a22fccabaae24186b92389f8', 'text': "Let's look at the new threat surfaces that are introduced by energy networks utilizing 5G technology. Figure 9-14 illustrates an example of a 5G use case deployment for an energy utility company.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 638, 'parent\_id': '4e5fbbddf7e33605d89c0728c0f5b96e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '77b1326b48ddbd15ae33d86d9db86fab', 'text': '5G NFs (3GPP & non-3GPP) CM, PM, FM =10 Analytics Public Cloud & Interne /\\® | ( A)) 2 /N8 > gN\\B % i Power Generation - 30 Muttiple sources () Energy Consumer Energy Distribution Energy Generation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 638, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fef337773fe7b0b7873755597b812a03', 'text': 'Figure 9-14 5G Use Case Example for the Energy Utility Sector', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 638, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '268aa2ccfd43aabbd3d6821eac139740', 'text': 'The key components of the energy utility use case shown in Figure 9-14 are explained in the list that follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 639, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8dfaa0b0986f198855358d255d48ea04', 'text': '1. Smart sensors in energy generation plants: These smart sensors are capable of listening and connecting to 5G radio nodes. These will be connected to on-premises equipment in the energy/power generation plants to monitor the critical infrastructure. Some of the use cases for these smart sensors in the location will be for monitoring the key statistics of critical infrastructure and sending it across to the centralized monitoring system.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 639, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9b387e2c74092130ce523d75adc9e06c', 'text': '2. Smart sensors in the energy distribution centers: The smart sensors in energy distribution locations are capable of monitoring and identifying critical outages in real time. This enables you to resolve outages much faster.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 639, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e4059d7ea0d7f05d69c1e7030581ac5b', 'text': '3. Smart sensors in customer locations: The smart sensors in customer locations will collect the real-time information of energy usage and send it to the centralized monitoring system for customer on-premises equipment. This allows you to provide more tailored solutions to your customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 639, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '86e9cbcc2e4ffd3dfe79874963400020', 'text': '4. 5G gNBs: 5G radio nodes (gNBs) in different form factors such as software radios, split gNBs such as Distributed Unit (DU) and Centralized Unit (CU), macro cells, micro cells, and pico cells could be used to provide radio coverage to the sensors deployed by the energy utility company. The radio nodes could be part of the private network, also called a non-public network, that is deployed and owned by the energy utility company.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 639, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2cfdd4cb37a153901dd140cf0371a9bc', 'text': '5. 5G multiaccess edge compute (MEC): 5G MEC consists of 3GPP and non- 3GPP network components required to cater for the use case. There are different ways to achieve these use cases. For example, the state-owned energy utility company could deploy its own private 5G network, which includes 5G radio nodes in different form factors, back haul, 5G packet core, and integration with third-party applications for analytics and fulfilment of specific use cases such as performance monitoring and resolution. MEC, as described in Chapter 5, “Securing MEC Deployments in 5G,” can be deployed in public cloud, on-premises, or hybrid deployment mode. The NSaaS model could also be used if the energy utility company would like to reuse the service provider infrastructure. NSaaS is one of the key use cases being considered by service providers to monetize their 5G network deployments. The service provider, depending on its capabilities, could also offer to secure the IIoT network deployment, which might be deployed at the energy generation plants.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 639, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a9c977d169dce8e26b73a584c4ffff65', 'text': 'Figure 9-15 illustrates an example of the NSaaS model being used by the energy utility company.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 640, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '2a6a5df3df9831ec68c1f0d3bbc5f608', 'text': "Slice Service Creation & SLA , e S e e ey Management | | Managementfor Service Layer Energy Utiity Company Sensor AAA 4 solution evice lS\\I/i\\cAeD Senvice Creation e Network Slice & Slice subnet specific requirements API | B T T T Orchestration and SDN Layer E E S R e 5G NF speciic AP requirements | senmssnsbecanan Uty CEEET 3 's([oT) Ko LW Sice @ Sie2 Nescccccsananas Sl 2 m LLLLLLITTIELEY Y e-ProvIder ibers (MBB) ; E", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 640, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8411ea88b0b266eba145b81ddf4a0dd6', 'text': 'Figure 9-15 5G NSaaS Deployment Model for Energy Utility', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 640, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2427e3e841a6e6f6e25dc4d701831193', 'text': 'Figure 9-16 illustrates the private network deployment model being used by the energy utility company.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 640, 'parent\_id': '8411ea88b0b266eba145b81ddf4a0dd6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '4da67e953421ab88eb020899c45cc31f', 'text': 'g g Energy Utilty Private Network PCF, UPF, NEF, MEC Appln 0 5GC NFs - Public cloud & Internet i -ma K () A) g\\B Power DU+CU) Generation - Multiple source 5GC NFs - on-premises L SR ———', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 641, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3866389f322a7d0bcded4c552747ca92', 'text': 'Figure 9-16 Example of a 5G NPN Deployment Model for an Energy Utility', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 641, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67fa69cb02f310a51393512b916f883b', 'text': '6. 5G 3GPP and non-3GPP network functions deployed in the public cloud: This allows the energy utility company to be flexible in integrating 5G NFs with third-party applications for real-time analysis.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 641, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '75f11b8eeef13900911c8c984120a503', 'text': '7. When the NSaaS model is being followed, both the communication services provider (CSP) offering NSaaS and the communication services customer (CSC—in this case, the energy utility company) consuming NSaaS have knowledge of the existence of network slice instances. Depending on service', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 641, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1acb82fd9cd3ec364a82cab047103b44', 'text': 'offering, the CSP offering NSaaS might impose limits on the NSaaS management capabilities exposure to CSC (the energy utility company). The CSC can manage the network slice instance according to the limited level of NSaaS management capabilities exposed by and agreed upon by the CSP.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 642, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e6370e6d8cdd25824fdf8c314181a2c1', 'text': 'Threats in the 5G-Enabled Energy Utility', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 642, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '153d7076f8c0fc7d6f29013c92663978', 'text': "Critical infrastructures such as utilities have been the subject of sophisticated cyberattacks aimed at data exfiltration, mapping critical infrastructures and collecting detailed information about them to create detailed targeted attacks. Apart from the attack surfaces, legacy control systems also pose multiple risks. The legacy, often proprietary, control systems are no longer efficient to operate and are challenging to secure. If not adequately detected and contained, cyberthreats can go on for a long time and impact networks, monitoring systems, and consumer smart sensors. Targeted attacks, such as crippling the targeted country's entire electric grid, can cause havoc and complete chaos.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 642, 'parent\_id': 'e6370e6d8cdd25824fdf8c314181a2c1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '163a7d43c08b0d033e4ae458eb929d03', 'text': 'This section will discuss the threat surface in the 5G deployment for the energy sector use case. The threats will cover different deployment models, such as private 5G deployment by the energy utility company and the NSaaS model. This section will cover the threat surfaces for the energy utility company and the service provider. Figure 9-17 shows the key threat surfaces for the manufacturing use case.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 642, 'parent\_id': 'e6370e6d8cdd25824fdf8c314181a2c1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ade81f1c08c520e8b8c363988f73ef5d', 'text': '+ CM, PM, FM layer atiack \* APl vulnerabilties & misconfiguration + Exploit vulnerabilities in smart sensor applications + Data exfilration \* Improper Access Control \* Improper Access controls i + Data exfilration + Host HW & OS vulnerabilities Publc Cloud & Intemet ¢ API vulngrabilties & misconfiguration \* Improper Slice configuration | Energy Provider o] ) NW — 5 — (= P=1 \* Improper Access Control N + Data exfilration + Smart sensor vulnerabilties + APl vulnerabilties and misconfiguration A ) + Denial of Service to sensors & S K\\ \* Improper Slice configuration + Sensor based DDoS atiacks ,\'z((A)) t", \* /I’ o8 \* £ oNB \\ \\ ! ! ! A 1 ! ! ¥ Power Generation - A \* ¥ %\* N— — Multile sources Energy Consumer Energy Distribution Energy Generation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 643, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fb10738700881c18b64336072976918e', 'text': 'Figure 9-17 Key Threat Surfaces for 5G Energy Utility Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 643, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4593d290cacb1a33efa705eccafe04cd', 'text': 'Inadequate Application-Level Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 643, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bff6b24081a3fcb6a1da58a7307cfbd6', 'text': 'All the 5G NFs are based on the cloud-native principles where the open source software stack will be used to build both 3GPP and non-3GPP Network Functions for 5G, which can then be deployed on the premises and in any public cloud offering.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 643, 'parent\_id': '4593d290cacb1a33efa705eccafe04cd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'adfe2e933c7add74f935907e88146bba', 'text': 'Specifically for the energy utility use case, one of the key threats at the application level is the unauthorized access of smart sensor configuration management deployed in the public cloud. If any attacker has unauthorized access to the configuration management, it can lead to complete control of the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 643, 'parent\_id': '4593d290cacb1a33efa705eccafe04cd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7ee24ea15d0e94f24eca7d46df55932d', 'text': 'smart sensors. The smart sensors can then be force-updated with a malicious code. The malicious code then can initiate a distributed denial-of-service (DDoS) attacks toward the 5G infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 644, 'parent\_id': '4593d290cacb1a33efa705eccafe04cd', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c718155d48af8b1d37ed44ec0df58269', 'text': 'API Vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 644, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a1ffddb2abfb9cea4d0b8d49cda42ec3', 'text': '5G brings in service-based architecture (SBA), which uses API-based communication between the 5G NFs. If the NSaaS model is used to cater for the energy utility use case, then the energy utility company can manage the network slice instance via the management interface exposed by the service provider using an API. APIs might also be used by the smart sensors to communicate with the MEC application to detect and respond to any disruptions in service in the energy grid. Although APIs enable many of the interactions in the energy utility use case, they also bring in risk vectors due to improper implementation of APIs and security misconfigurations.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 644, 'parent\_id': 'c718155d48af8b1d37ed44ec0df58269', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5b0f896610247eb2fc5a4554ede77b02', 'text': 'In NSaaS deployments, broken authentication of APIs can lead to unauthorized access to the slice management layer. This can lead to users from another slice accessing the management of the energy utility slice and deleting an entire slice subset. This can lead to loss of service or service outage.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 644, 'parent\_id': 'c718155d48af8b1d37ed44ec0df58269', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ae124b05ec4d1e56e7f4571d8e111763', 'text': 'Energy Provider Network Vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 644, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '247d505c7a513a2aae5d8d88f5c6741a', 'text': 'Improper isolation between the IT network of the energy utility company and the IIoT control network (through a smart sensor network, for example) can lead to attacks from the Internet or any malware from the IT network impacting the smart sensor network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 644, 'parent\_id': 'ae124b05ec4d1e56e7f4571d8e111763', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3fc3fd77eabfc7ba53671c5f5ff5d9b8', 'text': 'Host OS and hardware (HW) vulnerability is another threat vector. If the 5G energy utility use case deployment model consists of certain applications related to the smart sensors being deployed in the on-premises data center, it could be prone to side-channel attacks, leading to data exfiltration of sensitive data from the smart sensors.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 644, 'parent\_id': 'ae124b05ec4d1e56e7f4571d8e111763', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7ef25e99f4bc7a9ef8d941edbd3abf8b', 'text': 'Securing 5G-Enabled Energy Utility', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 644, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '47d2e815736c7c6085d0a361caccc49d', 'text': 'The energy sector is identified as one of the most critical national infrastructures by many countries. This sector must maintain stringent reliability and availability of the power grid. In countries like the US, standards like North American Electric Reliability Corporation – Critical Infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 644, 'parent\_id': '7ef25e99f4bc7a9ef8d941edbd3abf8b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8af5d9975b1fed3e23226e411212f8b1', 'text': 'Protection (NERC-CIP) are designed to secure the assets required for operating the electric system.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 645, 'parent\_id': '7ef25e99f4bc7a9ef8d941edbd3abf8b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3ebac48d064bcd1e7ae1936e74256286', 'text': 'While 5G does help in optimizing the total cost of ownership (TCO) by implementing innovative and effective use cases, it also brings in new risks. This section discusses the multilayered security controls to secure critical energy sector 5G use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 645, 'parent\_id': '7ef25e99f4bc7a9ef8d941edbd3abf8b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5b38ba8b6d2d3dcbe85310616107316a', 'text': "Securing 5G critical infrastructure use cases such as energy utility requires a holistic approach rather than just focusing on securing the 5G components. This is because the energy sector has been in operation for quite some time, and the 5G IoT/IIoT network will require integration with the legacy network. This integration is important because 5G use cases should complement the existing legacy framework to help you achieve cost optimization. Ripping out the legacy infrastructure is not always the right decision. It looks attractive in PowerPoint slides, but implementing a full overall “rip and replace” inherently has a lot of unforeseen challenges, leading to delay in the project or adding more complexity and cost. Let's discuss some of the key areas to secure and look at re-utilizing and enhancing the existing technology and infrastructure.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 645, 'parent\_id': '7ef25e99f4bc7a9ef8d941edbd3abf8b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd441090039e11c65795c22822511effa', 'text': 'Looking at the energy sector, network transformations, transmission, and especially distribution involves investing in digital technology that is transforming the grid. IT and OT convergence are also transforming the utility market, requiring a blend of technology and expertise from both organizations to optimize the benefits of digitizing the utility. You should segment the operations environment, detect suspicious traffic flows and behavior, perform security policy audits and detect violations, and identify compromised devices. Across this security posture, automation is fundamental to facilitate the scale required in an OT environment. Further, utilities can reduce risks across all OT and IT traffic by creating visibility into how, when, where, and why users and devices connect to the network. Apart from multilayered security controls, you should work closely with your suppliers and ecosystem of industrial partners to deliver secure devices and deploy networks with best practices in mind.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 645, 'parent\_id': '7ef25e99f4bc7a9ef8d941edbd3abf8b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b6015d21dbefbe9381b28cb06d3cca9a', 'text': 'Figure 9-18 shows the key security controls for mitigating the threats for the smart sensors within the energy utility use case.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 645, 'parent\_id': '7ef25e99f4bc7a9ef8d941edbd3abf8b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '777580bbffc0597d0e382b2e57c4b59b', 'text': '- - 0 onfiguration Management & A (coess Control - E - - / " \* Transmission Distribution System @ 1 Secure Fault Management & 0DoS protection by Communication SCR Performance Management (IPsec / TLS - based on capabilty and \\ Use case) — [0 ( MEC/56C |¢ ’((A)) gNB Secure Connected Grid Router (S-CGR) Secure Zero-Touch Provisioning & on- Encrypted using TLS/IPsec depending on device capabilty boarding @ \\ / ~ On-premises or v’ public cloud 0 U ! o WK Smart Smart Load Transformer Distribution Power Generation Meter Lights Control Monitoring RTU for FM Monitoring', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 646, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6a5fad8c47698da79444446ed12a52e9', 'text': 'Figure 9-18 Key Security Controls for Energy Utility Being Catered by 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 646, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2bf36ef50cc4a693e1bb78ec1c58a77c', 'text': 'The list that follows explains the key security controls illustrated in Figure 9-18 in more detail:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 646, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'acd6cee0eea4275676e09491a977d8b9', 'text': '1. The Secure Connected Grid Router (S-CGR) enables secure connection to all the smart sensors deployed in various parts of the energy utility network. Depending on the capabilities of the sensor, the S-CGR would use TLS, IPsec, or any other mechanism to secure the communications with the smart sensor. The S-CGR should support Supervisory Control And Data', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 646, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6b025585b1e8b52cb49ee4a71db945af', 'text': 'Acquisition (SCADA) protocol (serial-to-IP) translation features to allow easy integration of legacy (non-IP) devices onto an IP network. It should also support integration with Advanced Smart Metering, Distribution Automation, Remote Workforce Automation, as well as integration of Distributed Energy Resources (DER) and secure wireless console access for remote access and resolution of critical faults.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 647, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '81977b29985964ea885b0779923eb707', 'text': 'The S-CGR should also support integrated Global Positioning System (GPS), which will help with location mapping of the router. S-CGR should provide network segmentation and quality of service (QoS) features, allowing logical separation of application traffic with specific constraint policies applied on each traffic flow.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 647, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f0ce62426546b0a803dad409ed6159d', 'text': "2. To allow authentication of the sensors and users, S-CGR should have integration with the user and device identity and management solutions, PKI infrastructure as well as allow Secure Zero-Touch Provisioning (S-ZTP). S- CGR should support mutual authentication and authorization of all nodes connected to the network, IEEE 802.1x-based authentication, role-based access control (RBAC) and certificate-based identity, and strong usernames and passwords. S-CGR should allow tamper-proof secure storage of router configuration and should use a hardware chip to store the router's X.509 certificate and other security credentials.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 647, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d77ab9556c1a559aa60127dcebbce3a', 'text': 'The smart sensors being used in critical infrastructure deployments should allow S-ZTP Day 0 configuration options, include a tamper-resistant mechanical design and generate security alerts if compromised.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 647, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '97814330735f35d34896d019c3f25e4c', 'text': '3. The transmission distribution system includes fault location isolation and service restoration (FLISR), SCADA, and analytical layers to provide real- time analysis of any disturbances, enabling quicker and accurate identification of faults.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 647, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '259f619d2b625c8ad0ad0f576d0061ff', 'text': '4. The analytical layer should include the closed loop anomaly detection, which can identify any anomalies in the network using telemetry from various components of the architecture, such as network telemetry from switching and routing devices, hypervisor metadata, container telemetry, and so on. The anomaly detection solution should be able to recommend appropriate action to mitigate any identified threat. For example, the analytical layer could identify the anomalies in the smart meter behavior, such as the smart meter device trying to reach out to an unexpected url. Such behavior could indicate that the device has been compromised. An appropriate action that the closed loop anomaly detection system could', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 647, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b4f0e8d76b1201115c3b5134f554fd45', 'text': 'recommend is to isolate the device by allowing access to only a quarantine network. Once the device is inspected and seen to comply with the security policy, it can be introduced back to the non-quarantine part of the network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 648, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '03e0dac2241121fd7a10df983dfb2b49', 'text': '5. The communication between the network devices and the transmission distribution system should be secured using secure mechanisms such as TLS or IPsec.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 648, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '24a00a993a4a0c6bb4a223bf503d3950', 'text': '6. With regard to secure connectivity toward 5G, to mitigate the DDoS attacks against the 5G network, S-CGR will include rate-limiting mechanisms.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 648, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9ba3cff81684530e88eb68163dd1893e', 'text': 'Figure 9-19 shows the summary of security controls for securing the critical energy sector 5G deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 648, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5c68900c1e9ac298cd94a6429c0e2962', 'text': 'Public Cloud & Internet —F8— = /\\ W A NB \* A)) >\\\\ \*I,’g gNB Power Generation %ﬁr —»r P Multiple sources Energy Consumer Energy Distribution Energy Generation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 649, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f50471fc24e51e707f2d32e01b120c70', 'text': 'A', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 649, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '94d0784be6355323183b3c3ef9a6542a', 'text': 'o, e ey', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 649, 'parent\_id': 'f50471fc24e51e707f2d32e01b120c70', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '12651353316832e28fb099c61f2581c9', 'text': 'Figure 9-19 Summary of Security Controls for Securing Energy Utility Sector', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 650, 'parent\_id': 'f50471fc24e51e707f2d32e01b120c70', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'text': '5G Vehicle-to-Everything (5G-V2X)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 650, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dcb3aa0f8bca7d6d236a11bb8f99c635', 'text': 'Innovations in connected vehicles with the vision of autonomous transport systems requires an infrastructure that can provide high throughput for in-car infotainment and ultra-reliable and low-latency services for assisted driving. In addition to existing IEEE 802.11p and dedicated short-range communications (DSRC) technology, 5G promises to deliver reliable, real-time communication at high speed on the distributed architecture needed to support transmission between vehicles, network, and transport infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 650, 'parent\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5db8334858b4393e2f1a40a9f140bd0d', 'text': 'Vehicle-to-everything (V2X) communication enables data exchanges between vehicles, infrastructure, pedestrians, and applications running on the edge and cloud. The different types of V2X are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 650, 'parent\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b5619dd0fa9a7503b7191bf7880016d4', 'text': '• V2V: Vehicle-to-vehicle', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 650, 'parent\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '101443684f8bc875f4c08f04f355817c', 'text': '• V2I: Vehicle-to-infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 650, 'parent\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '30ec2e21567ed4ed3b6a70db9db60df7', 'text': '• V2P: Vehicle-to-pedestrian', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 650, 'parent\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bd9dc6228007b4d40d6006977312cc54', 'text': '• V2N: Vehicle-to-network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 650, 'parent\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9beefc77bbdc0277de10e07d0e239004', 'text': '• V2S: Vehicle-to-sensor', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 650, 'parent\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c15bf96c654e768c353d8cdaac377945', 'text': 'V2V, V2I, V2S and V2P are short-range, direct device-to-device communications and can exist without 5G coverage. To enable these type of communications, 3GPP has specified the PC5 reference point/interface.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 650, 'parent\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '62c19fe0ea907a20b02e4d2d9c821800', 'text': 'V2N is device-to-network communication utilizing 5G networks. To enable V2N communications, 3GPP has included attributes related to V2X in the specifications for UE, air interface, and 5GC NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 650, 'parent\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e89a59d2e22ea719ed649fe4a7c1e0d4', 'text': 'Figure 9-20 illustrates the non-roaming 5G system architecture for V2X communication over PC5 and Uu reference points as specified in 3GPP TS 23.287 V16.5.0.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 650, 'parent\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8f76aa33c3b151e3e1c28d9cfcc3137e', 'text': 'In order to simplify interworking, interoperation, and interchange among different stakeholders, 3GPP has specified V2X Application Enabler (VAE). VAE will allow common functionalities to be utilized by different V2X applications, including the network situation and QoS monitoring,', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 650, 'parent\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f0757b87830dbafe8c38eb5e6f407f8c', 'text': 'communication parameter (for example, PC5), and network resource management.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 651, 'parent\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '60d6cfa8369e2c450e55239bcdaf2a37', 'text': 'Apart from VAE, 3GPP has also specified the Service Enabler Architecture Layer (SEAL) in order to support vertical applications over the 3GPP system.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 651, 'parent\_id': '1ba688e07432dce08c96cb2e8d1332fb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd0a840fe703073e77ee6b959e10c0025', 'text': 'Data Network VX Application UDM PCF NEF Server N NRF UDR AMF SMF UPF NG-RAN Uu Uu UEA UEB [~ PC5 PCS Vb V5 V1 JGPPTS 23,287', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 651, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '420e91be1fa31cb132fbf4d9fb7d4fac', 'text': 'JGPPTS 23,287', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 651, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '518365f01de858b4b833ec3108e42585', 'text': 'Figure 9-20 Non-Roaming 5G System Architecture for V2X', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 651, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '426e5b88c3f7e7be35a49a7774754dac', 'text': 'Figure 9-20 Non-Roaming 5G System Architecture for V2X Communication', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 651, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'facd88a90dff385a1574999add1ee0ad', 'text': 'The interfaces in Figure 9-20 are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 651, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d2689e1a9a1acc5123e0bc5a299d4a8', 'text': '• PC5: Interface specified for V2X between the UEs. It includes the LTE- based PC5 and/or NR-based PC5. The PC5 reference point will use the Hypertext Transfer Protocol (HTTP), Message Queue Telemetry Transport (MQTT), or Advanced Message Queuing Protocol (AMQP).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 652, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a15dca196d1292e8c962aeffc5aae1e4', 'text': '• Uu: Interface between UE and NG-RAN (gNB).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 652, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e3b8e6798bd520988949902806c0160e', 'text': '• V1: Interface between the V2X applications in the UE and in the V2X application server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 652, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '986dc79577be5fe28c571fb0e7d80b70', 'text': '• V5: Interface between the V2X applications in the UEs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 652, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '49d2fc7e704dcb59fc814f1be4ef00d6', 'text': 'Apart from the preceding interfaces, the following interfaces and NFs will carry additional messages to enable V2X services:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 652, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '61dc13b48a5962ce938e6a0ab35c29ff', 'text': "• N1 interface between UE and AMF will be used to convey the V2X policy and parameters (including service authorization) from AMF to UE and to convey the UE's V2X capability and PC5 capability for V2X information from UE to AMF.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 652, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '86c57a55699aaafd5ce4bc0a3b59b526', 'text': '• N2 interface between NG-RAN and AMF will be used to convey the V2X policy and parameters (including service authorization) from AMF to NG- RAN.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 652, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e92837c8bf93744404b78b4d1318cdaf', 'text': '• NEF services are used to enable communication between the 5GC 3GPP NFs and non-3GPP V2X application server NFs, as shown in Figure 9-21.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 652, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '28bf502d9271feb67a8d62d9565d29ad', 'text': 'Data Network V2X AP| Application server > N37 NEF N30 5GC UDR N36 PCF N15 AMF N2 N1 Uu UEA V2x U Application 3GPP TS 23.287', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 653, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bd71d835a0ab7fffce6581fc1ab48a3b', 'text': 'Data Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 653, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0cb32299c882a035441da08b40c40965', 'text': '3GPP TS 23.287', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 653, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f68e1dc7d484982c5ab3ceb1def1168d', 'text': 'Figure 9-21 High-Level View of AF-based Service Parameter Provisioning for V2X Communications', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 653, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dc80ce22f817a76569e2c070dd30d0b9', 'text': 'Figure 9-21 shows the high-level view of AF-based service parameter provisioning for V2X communications. The V2X application server may provide V2X service parameters to the PLMN via NEF. The NEF stores the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 653, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dd16d81aec6aec734084e6734fe69c90', 'text': 'V2X service parameters in the UDR. The 5GC reference points N37, N36, N30, and N15 shown in Figure 9-21 are all API-based service-based interfaces (SBIs). The V1 reference point will use HTTP or MQTT.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 654, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f63481657f91013f5c03922476575dc9', 'text': '5G allows convergence of 3GPP and non-3GPP networks to 5G packet core (5GC), thereby allowing the coexistence of multiple technologies enabling V2X use cases. 5G enablers such as MEC, network function virtualization (NFV), network slicing, API-enabled SBA and open software, stack-based Cloud-Native Functions (CNFs) will help you realize V2X use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 654, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6f80e4bca938dba9a68a80a1e173bfc1', 'text': 'V2X will include use cases that impose varying latency requirements. For example, use cases such as real-time awareness would require URLLC with stringent high-availability requirements. V2X will also include use cases such as video streaming, as an in-car entertainment service, which requires high- bandwidth but lower criticality. 5G allows networks to move away from monolith mode of network deployment to a flexible virtual network deployment with resources being allocated based on the use case requirements using network slicing, as shown in Figure 9-22. 5G networks will use MEC to deploy the low-latency dependent non-3GPP applications and 3GPP NFs closer to the edge in the public cloud or on-premises regional/micro/mini data center. NFV, augmented by software-defined network (SDN) and orchestration, allows optimum distribution of NFs using Control Plane User Plane Separation (CUPS), optimum sharing of resources, and allows scalability based on actual capacity and performance requirements, thereby making the network more flexible and dynamic for different types of services.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 654, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'cbe739c68590ad1ff3f182e0fe601005', 'text': 'VX Applton — S8 1 Slice 2 Slicg 3 @0 Public Cloud & Internet Uom NRF PCF NEF NSSF SMF AMF 2 AMF3 SMF3 VX UPF3 08M Slice 1- VX Application Appln i UPF1 (y) Centralized 5GC — & Sics - Seaning Slicg 3 - Configuraton, Fault & Performance Momt MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 655, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd3d4812ae16d357978975b0721417c3f', 'text': 'Figure 9-22 Example of 5G-V2X Deployment Utilizing Network Slicing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 655, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '35533d7cd4eb2b9b9dc024b783a98e9e', 'text': 'Figure 9-22 depicts the slices configured:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 655, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c4e28898fe595fbae8a2404c994ea744', 'text': '• Slice 1 is the URLLC slice, which is latency sensitive and has low- bandwidth requirements', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 655, 'parent\_id': '35533d7cd4eb2b9b9dc024b783a98e9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '51483b3a921360b986bafdcefbdd3226', 'text': '• Slice 2 caters for in-car entertainment and has a requirement on high bandwidth and has less-stringent requirement on latency.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 655, 'parent\_id': '35533d7cd4eb2b9b9dc024b783a98e9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '72f0f2718d1e824d82caeba430ac80ac', 'text': '• Slice 3 caters for configuration, fault, and performance management, requires low bandwidth, and is not very sensitive to latency.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 655, 'parent\_id': '35533d7cd4eb2b9b9dc024b783a98e9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '252651b3b364e75adbdbd3b79586c554', 'text': 'Applications that are latency sensitive, such as V2X MEC applications, are deployed in the edge of the network. They interact with the V2X applications in vehicles and direct them to the specific V2X application servers deployed in the public cloud in this example. Applications that are not latency dependent,', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 655, 'parent\_id': '35533d7cd4eb2b9b9dc024b783a98e9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '37339de5a9c1b1a8947e2c9608d0b08d', 'text': 'such as applications for operations and maintenance, and 5G control plane NFs are deployed in the centralized 5G Core data center.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 656, 'parent\_id': '35533d7cd4eb2b9b9dc024b783a98e9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b05da0f8fa95e90feeca239ba42affa2', 'text': '5G-V2X can be used in multiple ways to enhance road safety. Some of the key 5G-V2X use cases are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 656, 'parent\_id': '35533d7cd4eb2b9b9dc024b783a98e9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '08ab0ccde11d8cb30e308a572b03c6e1', 'text': '• Real-time awareness: Real-time awareness will enable vehicles to receive real-time information about speed recommendations based on traffic conditions and weather information, lane closures, traffic density, accident alerts, and other conditions that might necessitate adjustments to driving patterns. This 5G-V2X use case requires extremely low-latency communication, which is allowed by MEC deployment bringing the low- latency-dependent applications closer to the edge. Network slicing can be used here to reserve the required resources to allow real-time awareness, as this is a critical use case that requires high availability.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 656, 'parent\_id': '35533d7cd4eb2b9b9dc024b783a98e9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da7eea046008b09f1224df22cc39dfe9', 'text': '• Intent-based driving: Vehicles driving in proximity can share information with each other for activities such as lane changes, sudden stops, and so on to avoid collisions, improve traffic safety, and increase efficiency. Similarly, traffic information can be collected from roadside units, temporary roadwork blocking units, and pedestrians for vehicles to obtain a holistic view of the driving environment, making it increasingly autonomous.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 656, 'parent\_id': '35533d7cd4eb2b9b9dc024b783a98e9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f0524dd68c8137bc8022bef4d9ae5f0', 'text': '• Edge and cloud integration: V2X applications on the UE, such as vehicles, will need to use network resources available at the edge for CDN caching content for improved quality of experience (QoE). V2X applications on the UE also require backend integration with the V2X application servers and cloud-hosted, backend systems to provide vehicle- to-network application services over the licensed cellular spectrum. Such applications require centralized control to operate the service subscription management necessary to enable vehicles to securely create a trust group with other vehicles in order to form a platooning convoy and have trusted data exchange. In addition, V2X applications, such as road safety, traffic management, and infotainment services running on the core, cloud, and third-party infrastructure, need secure management to ensure critical real- time information legitimacy. Trusted vehicles can subscribe to OEM services and third-party services for functionality updates, such as a new map for navigation, with a dynamic API interface allowed by the Network Exposure Functionality (NEF) on the core.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 656, 'parent\_id': '35533d7cd4eb2b9b9dc024b783a98e9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b0f504bc37e896f3f3d1eb9330292918', 'text': 'Figure 9-23 illustrates an example of V2X deployment, with the NSaaS model being utilized by the communication slice consumers (CSCs). The slices are being consumed by multiple entities, such as the car manufacturer, road policing unit, traffic management center, and media and entertainment for vehicles.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 657, 'parent\_id': '35533d7cd4eb2b9b9dc024b783a98e9e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'e66c0df1bfa0740d0f6dcc5b03863023', 'text': 'Roads Policing Unit [P VX AP 1 Application API&N6 2o Public Cloud & Internet UDi NRF PCF NEF NSSF API & NG SMF | AN —r— a VX UPF3 O&M % A Slig 1-V2X Application Appin 5&V5 — UPF1 Siice 2+ Streaming data ) Centralized 5GC —\_— — Slice 3 - Configuration, Fault & ( A) Performance Man ak (. MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 657, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ededc98954cb9feb5a6808cda71f6116', 'text': 'Figure 9-23 5G-V2X NSaaS Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 657, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '54982b626162a4dcddf462b9724aac37', 'text': 'Threats in 5G-V2X Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 657, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cdbef9f4d6f7e1590959c67b34dfc6d8', 'text': '5G-V2X enables both safety and non-safety vehicular-related use cases. Many of the use cases, specifically safety related, require low latency and high reliability, and because they are classified as URLLC use cases, they will be susceptible to the following risks:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 658, 'parent\_id': '54982b626162a4dcddf462b9724aac37', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a7cf6a519b06c48d11aaf123a319e6b2', 'text': '• Service availability and DoS to critical services such as road policing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 658, 'parent\_id': '54982b626162a4dcddf462b9724aac37', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '378a960012e4ade9243cd54939140709', 'text': '• DDoS attacks from V2X devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 658, 'parent\_id': '54982b626162a4dcddf462b9724aac37', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '01bf28f2792b04b5cb91f3da3284136b', 'text': '• Data exfiltration of sensitive user and device information', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 658, 'parent\_id': '54982b626162a4dcddf462b9724aac37', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '47f64eaab7badb3feab2747facbee977', 'text': '• Improper identification and access control of users and devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 658, 'parent\_id': '54982b626162a4dcddf462b9724aac37', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd7bdcb09a78abea358e9580e23dc80bd', 'text': 'This section will take you through some of the key threat surfaces in 5G-V2X deployment, illustrated in Figure 9-24.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 658, 'parent\_id': '54982b626162a4dcddf462b9724aac37', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '77e6b10f44656c65c37e9484c61dd1bc', 'text': "0 Eavesdropping atiack using Mith at PCS and V5 interfaces 0 Malicious code injected into vehicle OBU during firmware update 0 Trafic Management Center 0 Malicious code injected into V2X application during application updates Weak inbuit security 0 Improper access security In-Vhicle Media and 0 DDoS attacks towards 5G nefwork API Entertainment Applcaton API & N6 280 Public Cloud & Jatérnet APl Vulngrabilties 0 RF PCF NEF 39 Unauthorized sevice configuration ' Unauthorized routing configurations on slice components 0 API & N6 ANF 1 SMF 1 Malicious code injections from any of the network slice towards the vehicles and pedestrian network e SWF2 ANF 3 SWF 3 VX UPF3 08M - B 3 A Slice 1- V2X Application Appin 5&V5 ——— Centralized 56C \\ —— Slice 2- Streaming data . ’ ’ Sl 3- Configuraton, Fault & ((A))\_ k Pedormance Mon UPF2 L o MEC + Improper slce level authentications", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 659, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8bbcdd324daf4c9151082c81904ed888', 'text': 'Figure 9-24 Illustration of Key Threats in 5G-V2X Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 659, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '252c59b2a0042fc8d8e6b5c0cd1d4b72', 'text': 'The key threat surfaces for the 5G-V2X deployment shown in Figure 9-24 are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 659, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7864f3c205c31461f5d4d584d551b3f3', 'text': '1. UE communication with 5G RAN is prone to threats such as weak built-in security of the onboard units (OBUs), which can be retrofitted to vehicles for aftermarket deployment or factory-fitted in cars with V2X capabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 659, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f9b3ed116afcad222d69405be07c5a1c', 'text': 'One of the key risk vectors here is the malicious code that could be used as a forced OBU firmware update. Once the malicious code is installed, it will take control of the OBU. The attacker can now force the OBU to send out sensitive information to the command and control (C2C) server, which can then be used for detailed targeted attacks. If the malicious firmware code is mass-updated on the vehicles using the vulnerable OBU, the attacker can initiate a DDoS attack toward the 5G network. V2X applications can be attacked using the same concept, as shown in Figure 9-25. The V2X applications installed on the UE are also prone to vulnerability in the programs made to build the V2X application. The vulnerabilities can be exploited by the attacker to exfiltrate sensitive information.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 660, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd0a3e44f3e6f013379d0744a88a4c164', 'text': 'Another risk vector at this layer is the possibility of the rogue UE providing incorrect information to deceive other UE, which might trigger unnecessary actions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 660, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '816aefaa5823179d1599904c9d31ae26', 'text': 'a V2 application update with malicious code VX Application o API&N6 Update Public Cloud & Internet NR PCF NEF NSSF API & NG AMF 1 SMF 1 | AMF2 VX SHF3 ANF3 o Appin Malicious V2X VX UPF3 update 08M Appin 5&V5 Sleed-V2X Aplcaon UPF1 Slce 2- Streaming data (( )) Centralized 5GC — Siice 3 Configuration, Faut & Performance Man UPF2 P S MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 661, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd04b7fd751af9dd38e2541dd5219f057', 'text': '5&V5', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 661, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9b93b5370c95cc400bc70de3f5ee11de', 'text': 'MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 661, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7f15f4a44091dd90f72927475b0ea418', 'text': 'Figure 9-25 Example of V2X Application Being Updated by a Patch Embedded with Malicious Code', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 661, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6c7d473b913231e2f168b0434d04d843', 'text': 'As shown in Figure 9-25, the attacker can exploit the vulnerabilities in the V2X application to insert malicious code as an update and push it to all the endpoints for V2X application update. Once the endpoints are updated with the malicious code, they can be controlled by the C2C server operated by the attacker. The attacker can then launch a DDoS attack toward the 5G infrastructure operated by the 5G-V2X provider/service provider.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 661, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6eb3675a920e3368002a06c451dfe984', 'text': '2. Another area of risk is insecure API communication. For the V2X use cases to be realized, you will need to deploy the V2X application client and V2X', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 661, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5570adcc9f1fcd32f9e847210f9560d5', 'text': 'application servers. The V2X application servers will be deployed in multiple edge compute sites, which can be located on the premises or in the public cloud, as illustrated in Figure 9-25. APIs are also used in the NSaaS deployment mode, where different slice consumers or CSCs such as car manufacturer, road policing unit, traffic management center, and in-vehicle media and entertainment will require management access to the service layer for configuring QoS and other service-level parameters. Admins from the CSC will use APIs to communicate with the service-level management layer. The 5GC NFs are exposed to third-party application functions, such as the V2X application layer, using the API calls. So, as you see here, any vulnerability in the API could have a negative impact on the V2X deployment. V2X deployments will reuse the 5G API-based communications in the MEC layer. This includes the API calls being used by the NEF to integrate with the external network functions like the V2X application server. V2X will also require integration with many entities providing services such as media and entertainment services and entities providing emergency services such as road policing. Car manufacturers will also require connectivity to the vehicles to provide firmware updates. All the aforementioned management and services provisioning can be performed by integrating the entities with a services provisioning layer in network slicing deployments. The access to the management for the services will be provided using APIs. These APIs are prone to attacks due to vulnerabilities within the APIs and security misconfigurations during API implementation. Improper implementation of APIs will also lead to unauthorized access to slices, from which the attacker might be able to exfiltrate the data and, in worse-case scenarios, delete the all the network slice–related functions, leading to DoS to all the impacted slice users and devices. APIs also do not impose any restrictions on the size or number of resources that can be requested by the client/user. This can lead to DoS and to risks such as brute-', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 662, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3651afd7067284702edc6262b5383006', 'text': '3. Another area of risk in 5GC deployments is data exfiltration. This is due to the threats arising from improper authentication in network slice deployments, vulnerabilities in the host hardware and software, where 5G 3GPP and non-3GPP NFs are deployed, and vulnerabilities in the software components used to build the NFs. Chapter 7, “Securing Network Slice, SDN, and Orchestration in 5G,” covers threats due to networking slicing in more detail. To summarize the threats under this domain, the key risks arise from improper isolation of the NFs serving critical slices. As an example, if', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 662, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5a845e0f29e2681cefef875ad9d6b9ee', 'text': 'the NFs servicing critical slices (such as the road policing unit) are deployed in the same host hardware as the noncritical slices (such as in-vehicle media and entertainment), attackers accessing a noncritical slice could use the vulnerabilities in that slice to access the NFs in a critical slice and then exfiltrate sensitive data.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 663, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7320c8d9a9dd29598772c341d05f20bc', 'text': 'Securing 5G-V2X Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 663, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '26a734001070a4a8715de2e226f59ccd', 'text': '5G-V2X use cases are both safety related and non-safety related. While safety- related use cases are primarily URLLC, non-safety-related use cases are eMBB oriented and provide value-added services to consumers such as in-vehicle media and streaming. While 3GPP caters for securing V2X over an NR-based PC5 reference point, as specified in TS 33.536, and V2X over a Uu reference point based on existing secure Uu mechanisms, as specified in TS 33.501, there are general security and privacy principles applicable outside of the 3GPP scope that need to be secured by multilayered security controls. This section covers these multilayered security controls, which are summarized as follows::', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 663, 'parent\_id': '7320c8d9a9dd29598772c341d05f20bc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b6ab7fbeee54a9ee9d5f3708f8a0a504', 'text': '• Enhanced visibility: This layer should allow visibility for the control plane across the extended network, from the control plane on the V2X user equipment to the 5G packet core deployed on the premises and in the cloud. The enhanced visibility layer uses enterprise telemetry from the existing network infrastructure. It should provide advanced threat detection, accelerated threat response, and simplified network segmentation using multilayer machine learning and entity modeling. This layer should be able to provide you the capability to detect obsolete and insecure protocols. An example is the TLS protocols. Since their first iteration in 1995, SSL and TLS encryption protocols have had many versions. The most current version is TLS 1.3, which addresses vulnerabilities and supports stronger cipher suites; therefore, the older versions, such as TLS 1.1 and 1.2, should not be used. Network administrators need to be alerted when older versions are used on their networks. The solution chosen by you should create a baseline of the network and then allow advanced behavioral analytics, enabling you to know if any of the V2X-related slice NFs or V2X devices are behaving differently than usual. Figure 9-26 illustrates security controls for end-to- end monitoring, enhanced visibility, and patch management.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 663, 'parent\_id': '7320c8d9a9dd29598772c341d05f20bc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '2756dc97472c60e68bb8c6243792a56e', 'text': 'T et e Data Collection il 9 \* Vunerabitty Management v Palch management VX selmr — API&N6 e ! UDM NRF PCF NEF N¢ API & N6 AMF1 SMF 1 | SMF2 AMF3 SMF3 VX UPF3 N 08M . Siice 1+ V2X Application Appln PC5 &V ‘A UPF1 \\ Slice 2- Streaming data (( )) Centralized 5GC ’ ’ — ’ ’ ’ Slice 3- Configuration, Fault & 2 k m', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 664, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cfa3fd0d1cef9efe54fa7124916d9e71', 'text': 'Figure 9-26 Detection of Anomalous Behavior in V2X Applications in Control Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 664, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'af27ffb1faac0f48956ae326c02616b2', 'text': 'Control Plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 664, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '17ac8f4a13701ae6cda09de3f8e5e366', 'text': 'As Figure 9-26 illustrates, the end-to-end visibility layer should be able to provide you with end-to-end visibility, threat detection, and mitigation using the following listed functions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 664, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'adc418057e3f83adaddfb659a9f372cb', 'text': '1. Collect telemetry from different parts of your network, including cloud deployed NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 665, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4e50460c40e89e77beee7bb3a8e4ff79', 'text': '2. This should then be compared against the baseline of your network and the network security policy and be analyzed using ML and AI algorithms to identify any malicious traffic in the encrypted layer, specifically on external API calls from the 5G-V2X network to the cloud-deployed applications (specifically, for detecting any anomaly in the control plane).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 665, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '96b0c83779d9cf43e7d9fd2514485e73', 'text': '3. The data collected should also be analyzed to identify any vulnerabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 665, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5a783da96f2f460c832c3fc455ee2129', 'text': '4. Any vulnerabilities in the 5G 3GPP and non-3GPP V2X NFs should be patched. If the CNFs are container based, then the latest signed imaged should be downloaded from a trusted container registry to replace the existing container image with known vulnerabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 665, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e15eeffd60d2a8fbae80296de3f6c60b', 'text': '• Application protection and policy enforcement: A traditional perimeter- based security approach alone is ineffective in meeting the new 5G deployment modes to cater for V2X use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 665, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cb5773eee1bcc246d43e9fa073b3a5c1', 'text': '• To address these security challenges effectively, a new approach is required to define, discover, and implement a consistent security policy at different layers. When dealing with modern distributed and dynamic applications for V2X being deployed at public cloud and on-premises MEC, you need insight into applications and their dependencies. You also require the capability to apply business context and automation to core security policy management processes, such as change management, risk and compliance assessment, and auditing.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 665, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9c5dd23d2f90d0500804038b8e4434ec', 'text': '• You will need a combination of application policy discovery and workload-based enforcement with a mixture of infrastructure-based segmentation and be able to apply security controls for applications running in any infrastructure and any cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 665, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '31de0a759dda115e19ca0b051fc453a6', 'text': '• You must also be able to dynamically enforce granular microsegmentation policies on the workloads while providing a consistent, real-time policy for enforcement across infrastructure- based elements such as firewalls and the network. This will allow you to realize seamless security policy across a diverse multicloud environment, with the demands of any application, from static, legacy operating systems to dynamic container-based microservices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 665, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd0190eb7bb24b5c3feabb0c67fe58b6f', 'text': '• To generate an accurate microsegmentation policy, your chosen solution should perform application dependency mapping on the entire network to discover the relationships between different application tiers and associated services. In addition, the platform should be able to simulate the policy application pre-enforcement to ensure ongoing application availability. The normalized microsegmentation policy should then be enforced through the application workload itself for a consistent approach to workload microsegmentation across any environment, including virtualized, bare-metal, and container workloads running in any public cloud or any on-premises data center. Once the microsegmentation policy is enforced, the solution should continue to monitor for compliance deviations, ensuring the segmentation policy is up to date as the application behavior changes.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 666, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '45b9b81677d9350bde6b7c3d9a3da92f', 'text': '• You should also have comprehensive scanning capabilities, including build, ship, and run CI/CD pipeline scanning and vulnerability scanning during runtime. The solution should also review overall and individual risk scores for vulnerability exploits during runtime and be able to continually scan your container deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 666, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '842fcd8db3ecb6c430315efb93e1c996', 'text': '• API security: API security requires focus on multiple areas. Some of the key API vulnerabilities include the implementation of the API itself, where verbose error messages contain sensitive information such as the type and version of the web server being used. This requires proper validation of the error messages. As shown in the Figure 9-27, the APIs should be implemented with a robust API authentication mechanism, including standard authentication, token generation, and multifactor authentication. Best practices, such as denying all access by default, should be implemented as part of the access control mechanism. DDoS attacks from the V2X UE towards the V2X application servers can be mitigated using mechanisms such as rate limiting, payload size limits at the API layer, and ensuring that you configure limits on container resources at the configuration layer. Figure 9-27 illustrates security controls to secure API and user access.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 666, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'bf0763b36c221788d00611f7ca36acbd', 'text': 'Global Access Policy & Roads Policing Unit Granular [AM API GW | WAF In-Vehicle Media and API Entertainment VX ”m:”“—;\\PI&NG 20 API GW / WAF UoMm NRF PCF NEF NSSF API&NG SMF 1 SWF3 a VX 08M Appln 585 Y Slig 1-V2X Applcation UPF1 Slce 2- Streaming data (( )) Centralized 5GC — Slioe 3 - Configuration, Fault & Perfomance Mgm al MEC', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 667, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c71df0d966915ea30af29c28b61b68b9', 'text': 'Figure 9-27 Securing API and Providing Granular Access Control', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 667, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4fcd6aeb802c80a7884a2d6817ddc3fb', 'text': 'Figure 9-27 shows you the different locations within the 5G network to deploy the API gateway/API firewall to secure the API communication.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 667, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '89432e8d7fb7833981ba6641628f0b25', 'text': '• Enhanced access control: V2X deployment will use multiple vendors and contractors configuring the 3GPP and non-3GPP NFs. To prevent any malicious actors trying to access the system, apart from using role-based access control (RBAC) for the V2X NFs, a multilayered access control', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 667, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '57de0ff994cf7e9d8386a5ba7bc9901c', 'text': 'method using multifactor authentication and mapping of workloads to users is required to provide you with the right level of access control. The access control layer should also allow you to gain device visibility and establish trust with endpoint health and management status. Having an enhanced access control layer with adaptive and role-based access controls using the global policy, as shown in Figure 9-27, enables you to enforce access policies for every app.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 668, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'abb8ab6532725fc84e41e054d055bab9', 'text': '• Network security and anti-DDoS protection: For ensuring secured connections within the network, one of the key steps is to implement TLS encryption on all API communication between the V2X public cloud and on-premises MEC. Any traffic flowing through the untrusted public network should be secured using IPsec provided by a security gateway. Anti-DDoS mechanisms can be provided by multiple components. Anti- DDoS mechanisms could also be provided by built-in features in API GW/API firewalls using rate limiting and so on, which will cater for mitigations against brute-force attacks and botnets. Figure 9-28 shows the end-to-end multilayered security control to secure your 5G-V2X deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 668, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '893d158ee3030f731548e91c4802d6d4', 'text': 'VX API & N6 20 | UOM NRF PCF NEF NSSF API&NG ANF 1 SMF 1 AMF2 | SMF2 ANF3 VX UPF3 08M Appln 54 V5 A Siice 1- V2X Application Slice 2- Streaming data (( )) Centralized 5GC — Slice 3 Configuration, Fault & UPF2 Peromance Mgm! MEC Inbuilt HW & SW security Enhanced Visibility, Anomaly detection, Analytics & Monitoring Segmentation and Isolation Enhanced Access Control laver', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 669, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a564c61aa45a8dd05ad58f83c33accc1', 'text': 'Figure 9-28 End-to-End Multilayered Security Control to Secure your 5G-V2X Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 669, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b5da712bf2466c70f445dc82ef308d18', 'text': 'The aforementioned security controls, along with ongoing standardization efforts, are key for establishing a reliable and secure 5G-V2X solution. Solutions such as V2X would need integrations with many external non-3GPP functions, thereby requiring a robust multilayered security architecture, as illustrated in Figure 9-28. You might have realized by now that there are multiple standardization works, some still ongoing, such as 3GPP to ensure that 5G can really be used to realize V2X use cases. Enhancements to 5G-V2X capabilities such as the PC5 reference point show promise in the direction of', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 669, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1a20b647ffbfebb0372e42aa4a30aa53', 'text': 'real-world implementation on V2X. However, it seems there is still quite a long way to go to before mass deployments of V2X will be realized, as the business models or monetization models should also be dusted out before actual deployments take place.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 670, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '7bb8a882014d595e7cd8041e7d4c2a68', 'text': 'Standards and Associations', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 670, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a5d6c4d9a7f258fe008d432469e28d6', 'text': 'Adherence to the following standards will help you establish, operate, monitor, review, maintain, and continually improve the security posture of your 5G use cases. Note that the following list is not exhaustive and contains only a selected number of standards and associations that are of key relevance for secure 5G NPN deployments:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 670, 'parent\_id': '7bb8a882014d595e7cd8041e7d4c2a68', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '64050f6426b2e994380ad9ac7416717e', 'text': '• ISO/IEC-JTC1-SC27: The scope of ISO/IEC-JTC1-SC27 is the development of standards for the protection of information and ICT. This includes generic methods, techniques, and guidelines to address both security and privacy aspects, such as the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 670, 'parent\_id': '7bb8a882014d595e7cd8041e7d4c2a68', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f214d93753c0d0fe7692f36c13b8e212', 'text': '• A security requirements capture methodology', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 670, 'parent\_id': '7bb8a882014d595e7cd8041e7d4c2a68', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aa8204f936ae2d3dc49c1b447e6f225e', 'text': '• Management of information and ICT security; in particular, information security management systems, security processes, and security controls and services', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 670, 'parent\_id': '7bb8a882014d595e7cd8041e7d4c2a68', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '82a5ba9a3d2d2621a90c7a9cec55a211', 'text': '• Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity, and confidentiality of information', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 670, 'parent\_id': '7bb8a882014d595e7cd8041e7d4c2a68', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '27ac714942e5450f7cefabb8c0bb9aae', 'text': '• Security management support documentation, including terminology, guidelines, and procedures for the registration of security components', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 670, 'parent\_id': '7bb8a882014d595e7cd8041e7d4c2a68', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f3e9273570b93514ea18fc541bee45d7', 'text': '• Security aspects of identity management, biometrics, and privacy', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 670, 'parent\_id': '7bb8a882014d595e7cd8041e7d4c2a68', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8e7681bd88a3d7c3cc9a325295256d58', 'text': '• Conformance assessment, accreditation, and auditing requirements in the area of information security management systems', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 670, 'parent\_id': '7bb8a882014d595e7cd8041e7d4c2a68', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0625db6c317fad26b2c7a9fc34636d0e', 'text': '• Security evaluation criteria and methodology', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 670, 'parent\_id': '7bb8a882014d595e7cd8041e7d4c2a68', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ca7ddd6dac93bf59af91ca6b1006b9bc', 'text': '• ISA/IEC 62443: The International Society of Automation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 670, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '921e95fd6a12b6a1079a6bc31176a53d', 'text': '(ISA)/International Electrotechnical Commission (IEC) 62443 series of standards, developed by the ISA99 committee and adopted by the IEC, provides a flexible framework to address and mitigate current and future', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 670, 'parent\_id': 'ca7ddd6dac93bf59af91ca6b1006b9bc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7ae5dff3df1f9087d49874cf1d7209fb', 'text': 'security vulnerabilities in industrial automation and control systems (IACSs). The committee draws on the input and knowledge of IACS security experts from across the globe to develop consensus standards that are applicable to all industry sectors and critical infrastructure. A new standard in the series, ISA-62443-4-2, “Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components,” provides the cybersecurity technical requirements for components that make up an IACS—specifically the embedded devices, network components, host components, and software applications. The standard, which is based on the IACS system security requirements of ISA/IEC 62443‑3-3, “System Security Requirements and Security Levels,” specifies security capabilities that enable a component to mitigate threats for a given security level without the assistance of compensating countermeasures.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 671, 'parent\_id': 'ca7ddd6dac93bf59af91ca6b1006b9bc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6eda9538828b2e746ead2048ed5bd5b1', 'text': '• ISO27001: Information for implementing information security management system (ISMSs). Using them enables organizations of any kind to manage the security of assets, such as financial information, intellectual property, employee details, or information entrusted by third parties.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 671, 'parent\_id': 'ca7ddd6dac93bf59af91ca6b1006b9bc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58b98a5bddb25675f9958a5372a9a85d', 'text': '• FedRAMP: FedRAMP stands for the Federal Risk and Authorization Management Program. It standardizes security assessment and authorization for cloud products and services used by U.S. federal agencies. The goal is to make sure federal data is consistently protected at a high level in the cloud.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 671, 'parent\_id': 'ca7ddd6dac93bf59af91ca6b1006b9bc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9a48e05e92fead28a4c2d8f7a9053349', 'text': '• Secure Controls Framework (SCF): A comprehensive catalog of controls that is designed to enable companies to design, build, and maintain secure processes, systems, and applications. The SCF addresses both cybersecurity and privacy so that these principles are designed to be “baked in” at the strategic, operational, and tactical levels', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 671, 'parent\_id': 'ca7ddd6dac93bf59af91ca6b1006b9bc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5a5dc2a08cbd38b744492862c1cff462', 'text': '• NIST 800-53: NIST 800-53 is a regulatory standard that provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible and customizable and are implemented as part of an organization- wide process to manage risk. The controls address diverse requirements', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 671, 'parent\_id': 'ca7ddd6dac93bf59af91ca6b1006b9bc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '09e1333c073efd3925e558b63bef807f', 'text': 'derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines. Finally, the consolidated control catalog addresses security and privacy from a functionality perspective (that is, the strength of functions and mechanisms provided by the controls) and from an assurance perspective (that is, the measure of confidence in the security or privacy capability provided by the controls). Addressing functionality and assurance helps to ensure that information technology products and the systems that rely on those products are sufficiently trustworthy.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 672, 'parent\_id': 'ca7ddd6dac93bf59af91ca6b1006b9bc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e0629eb255471ba2e7d3d97c42a2e2db', 'text': '• NIST 800-82: NIST 800-82 is a regulatory standard that provides guidance on how to secure industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLCs), while addressing their unique performance, reliability, and safety requirements. It also provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 672, 'parent\_id': 'ca7ddd6dac93bf59af91ca6b1006b9bc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3e9a55714f937e8bb837705bebae792c', 'text': 'Due to the nascent stage of 5G NPN network implementations, other standard and partnership organizations, such as oneM2M, are looking at working closely together to focus on security and deployment aspects of IIoT for 5G SNPN and PNI-NPN deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 672, 'parent\_id': 'ca7ddd6dac93bf59af91ca6b1006b9bc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e4b76d52f324b26270a7ee0de2144ccb', 'text': "oneM2M is an association that constitutes by eight of the world's leading ICT standard development organizations: the Association of Radio Industries and Business (ARIB) from Japan, the Telecommunication Technology Committee (TTC) from Japan, the Alliance for Telecommunications Industry Solutions (ATIS) from the USA, the Telecommunication Industry Association (TIA) from the USA, the China Communications Standards Association (CCSA), the European Telecommunications Standards Institute (ETSI), the Telecommunications Standards Development Society, India (TSDSI), and the Telecommunications Technology Association (TTA) from Korea.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 672, 'parent\_id': 'ca7ddd6dac93bf59af91ca6b1006b9bc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ed2e1640968d61f3cca9ddb8ecca9b37', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 672, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2855f024cf45ef5e4fa9d008fabdf84', 'text': 'This chapter discussed the mechanisms for securing the key use cases being planned to be enabled by 5G. The use cases discussed in this chapter will require 5G-capable IoT/IIoT devices or IoT/IIoT devices capable of being', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 672, 'parent\_id': 'ed2e1640968d61f3cca9ddb8ecca9b37', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8297cf61571d1b8bd7914ae99d0eb90b', 'text': 'integrated with a 5G network gateway. Supply chain vulnerability is one of the key threats in the 5G use cases, specifically for the critical infrastructure use cases, as discussed in Chapter 8, “Securing Massive IoT Deployments in 5G,” in the section “Supply Chain Vulnerability.” The key methods to mitigate supply chain vulnerability are discussed in the same chapter, under the section “Securing Supply Chain.” The use cases definition is still in the nascent stages, and trials are being conducted with very low footprints.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 673, 'parent\_id': 'ed2e1640968d61f3cca9ddb8ecca9b37', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a4bff751f5a26b8e8d977bd2fa4f3cf', 'text': 'The key challenge most of the early adopters are having is the right design of also including the legacy infrastructure. If it was a greenfield deployment, it would be comparatively less complex because you need not consider the vulnerabilities in the older-generation equipment and workarounds, as implemented in network designs throughout ages of network implementations, migrations, and expansions. The security controls discussed in each of the use cases and adhering to the forementioned standards comprise a good starting point in your design for securing the 5G use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 673, 'parent\_id': 'ed2e1640968d61f3cca9ddb8ecca9b37', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4298618de1112ddc6c97c55e6934a258', 'text': 'Key Acronyms', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 673, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '77a9aceb79168246fe88826cf6e33b80', 'text': 'The following table expands the key acronyms used in this chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 673, 'parent\_id': '4298618de1112ddc6c97c55e6934a258', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '165282ce8f9e4ac312cf68626fd742e5', 'text': 'Acronym Expansion 5GC 5G Core AMF Access and Mobility Management Function ARIB Association of Radio Industries and Business ATIS Alliance for Telecommunications Industry Solutions AUSF Authentication Server Function C-v2X Cellular — Vehicle-to-Everything CCSA China Communications Standards Association CNF Cloud-Native Function Cobots Collaborative robots CSC Communication services consumer CSp Communication services provider DDoS Distributed denial of service DoS Denial of service DSRC Dedicated short-range communications ¢eMBB Mobile broadband', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Acronym</th><th>Expansion</th></tr></thead><tbody><tr><td>5GC</td><td>5G Core</td></tr><tr><td>AMF</td><td>Access and Mobility Management Function</td></tr><tr><td>ARIB</td><td>Association of Radio Industries and Business</td></tr><tr><td>ATIS</td><td>Alliance for Telecommunications Industry Solutions</td></tr><tr><td>AUSF</td><td>Authentication Server Function</td></tr><tr><td>C-v2X</td><td>Cellular — Vehicle-to-Everything</td></tr><tr><td>CCSA</td><td>China Communications Standards Association</td></tr><tr><td>CNF</td><td>Cloud-Native Function</td></tr><tr><td>Cobots</td><td>Collaborative robots</td></tr><tr><td>CSC</td><td>Communication services consumer</td></tr><tr><td>CSp</td><td>Communication services provider</td></tr><tr><td>DDoS</td><td>Distributed denial of service</td></tr><tr><td>DoS</td><td>Denial of service</td></tr><tr><td>DSRC</td><td>Dedicated short-range communications</td></tr><tr><td>¢eMBB</td><td>Mobile broadband</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 674, 'parent\_id': '4298618de1112ddc6c97c55e6934a258', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '0503599ec130e00678e622206e1c76de', 'text': 'ETSI European Telecommunications Standards Institute FLISR Fault location, isolation, and service restoration IAM Identity and Access Management IToT Industrial Internet of Things loT Internet of Things M2M Machine-to-machine MEC Multi-access edge compute MFA Multifactor authentication mloT Massive Internet of Things NF Network Function NPN Non-public network NSaaS Network slice as a service OBU On-board unit oT Operational technology PCF Policy and Charging Function PNI-NPN Public Network Integrated Non-Public Networks RAT Radio access technology RBAC Role-based access control RSU Road side unit S-CGR Secure connected grid routers SBA Service-based architecture', 'metadata': {'text\_as\_html': '<table><thead><tr><th>ETSI</th><th>European Telecommunications Standards Institute</th></tr></thead><tbody><tr><td>FLISR</td><td>Fault location, isolation, and service restoration</td></tr><tr><td>IAM</td><td>Identity and Access Management</td></tr><tr><td>IToT</td><td>Industrial Internet of Things</td></tr><tr><td>loT</td><td>Internet of Things</td></tr><tr><td>M2M</td><td>Machine-to-machine</td></tr><tr><td>MEC</td><td>Multi-access edge compute</td></tr><tr><td>MFA</td><td>Multifactor authentication</td></tr><tr><td>mloT</td><td>Massive Internet of Things</td></tr><tr><td>NF</td><td>Network Function</td></tr><tr><td>NPN</td><td>Non-public network</td></tr><tr><td>NSaaS</td><td>Network slice as a service</td></tr><tr><td>OBU</td><td>On-board unit</td></tr><tr><td>oT</td><td>Operational technology</td></tr><tr><td>PCF</td><td>Policy and Charging Function</td></tr><tr><td>PNI-NPN</td><td>Public Network Integrated Non-Public Networks</td></tr><tr><td>RAT</td><td>Radio access technology</td></tr><tr><td>RBAC</td><td>Role-based access control</td></tr><tr><td>RSU</td><td>Road side unit</td></tr><tr><td>S-CGR</td><td>Secure connected grid routers</td></tr><tr><td>SBA</td><td>Service-based architecture</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 675, 'parent\_id': '4298618de1112ddc6c97c55e6934a258', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'e8228a720dd7d7e644976bc813287c9b', 'text': 'SBI Service-based interface SCADA Supervisory control and data acquisition SDN Software-defined network SMF Session Management Function SNPN Standalone non-public network SSL Secure Sockets Layer TIA Telecommunication Industry Association TLS Transport Layer Security TSDSI Telecommunications Standards Development Society, India TTA Telecommunications Technology Association TTC Telecommunication Technology Committee UDM Unified Data Management UE User equipment UPF User Plane Function', 'metadata': {'text\_as\_html': '<table><thead><tr><th>SBI</th><th>Service-based interface</th></tr></thead><tbody><tr><td>SCADA</td><td>Supervisory control and data acquisition</td></tr><tr><td>SDN</td><td>Software-defined network</td></tr><tr><td>SMF</td><td>Session Management Function</td></tr><tr><td>SNPN</td><td>Standalone non-public network</td></tr><tr><td>SSL</td><td>Secure Sockets Layer</td></tr><tr><td>TIA</td><td>Telecommunication Industry Association</td></tr><tr><td>TLS</td><td>Transport Layer Security</td></tr><tr><td>TSDSI</td><td>Telecommunications Standards Development Society, India</td></tr><tr><td>TTA</td><td>Telecommunications Technology Association</td></tr><tr><td>TTC</td><td>Telecommunication Technology Committee</td></tr><tr><td>UDM</td><td>Unified Data Management</td></tr><tr><td>UE</td><td>User equipment</td></tr><tr><td>UPF</td><td>User Plane Function</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 676, 'parent\_id': '4298618de1112ddc6c97c55e6934a258', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '6a05e3d616043cc215a32e1a331ba234', 'text': 'V2I Vehicle-to-infrastructure V2N Vehicle-to-network v2p Vehicle-to-pedestrian V2§ Vehicle-to-sensor Vv Vehicle-to-vehicle V2X Vehicle-to-everything VNF Virtual Network Function SCF Secure Controls Framework NIST National Institute of Standards and Technology IACS Industrial Automation and Control System IEC International Electrotechnical Commission ISA International Society of Automation', 'metadata': {'text\_as\_html': '<table><thead><tr><th>V2l</th><th>Vehicle-to-infrastructure</th></tr></thead><tbody><tr><td>V2N</td><td>Vehicle-to-network</td></tr><tr><td>v2p</td><td>Vehicle-to-pedestrian</td></tr><tr><td>V2s</td><td>Vehicle-to-sensor</td></tr><tr><td>Vv</td><td>Vehicle-to-vehicle</td></tr><tr><td>V2X</td><td>Vehicle-to-everything</td></tr><tr><td>VNF</td><td>Virtual Network Function</td></tr><tr><td>SCF</td><td>Secure Controls Framework</td></tr><tr><td>NIST</td><td>National Institute of Standards and Technology</td></tr><tr><td>IACS</td><td>Industrial Automation and Control System</td></tr><tr><td>IEC</td><td>International Electrotechnical Commission</td></tr><tr><td>ISA</td><td>International Society of Automation</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 677, 'parent\_id': '4298618de1112ddc6c97c55e6934a258', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '05c5f05af3db206ade590f467570f681', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 677, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8768cefd13b81446b292f707294e35c8', 'text': '3GPP TS 33.536 V16.2.0, “Security Aspects of 3GPP Support for Advanced Vehicle-to-Everything (V2X) Services”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 677, 'parent\_id': '05c5f05af3db206ade590f467570f681', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bcd00d5ef943c1195f52dd0681764628', 'text': '3GPP TS 23.287 V16.5, “Architecture Enhancements for 5G System (5GS) to Support Vehicle-to-Everything (V2X) Services”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 677, 'parent\_id': '05c5f05af3db206ade590f467570f681', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'de448ac9fb9de49449fb2c41a40907d4', 'text': '3GPP TS 23.434 V17.1, “Service Enabler Architecture Layer for Verticals (SEAL)”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 677, 'parent\_id': '05c5f05af3db206ade590f467570f681', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ea6a1710ac3107b145012ff68f22250d', 'text': 'https://www.cisco.com/c/dam/en\_us/solutions/iot/demystifying-5g- industrial-iot.pdf', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 677, 'parent\_id': '05c5f05af3db206ade590f467570f681', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2022d7d3930daf5c728532e1520cd6d2', 'text': '5G Automotive Association, “C-V2X Use Cases and Service Level Requirements Volume II,” https://5gaa.org', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 677, 'parent\_id': '05c5f05af3db206ade590f467570f681', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '782e1e8cc803c2a98673be918a545627', 'text': '5GAA TR A-200094, https://5gaa.org', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 677, 'parent\_id': '05c5f05af3db206ade590f467570f681', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5e02f8a538ac599f636f2f865bb93c01', 'text': 'https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Solution\_ Briefs/IA\_Networking\_Solution\_Brief.html', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 677, 'parent\_id': '05c5f05af3db206ade590f467570f681', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bb9e9c75cd3453a7fda17e4a5ec76a2f', 'text': 'Pramod Nair, “ Securing Your 5G Infrastructure to the Edge and Beyond,” Cisco Live, Cisco Public, March 30, 2021', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 677, 'parent\_id': '05c5f05af3db206ade590f467570f681', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2e87cdaf673bdbab928031dababbef26', 'text': 'Pramod Nair, “Securing Your 5G Network End to End,” Cisco Live APJC, Cisco Public, April 30, 2019', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 678, 'parent\_id': '05c5f05af3db206ade590f467570f681', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bdd32e473abb291ff2c68d68e937de6f', 'text': 'https://www.isa.org/', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 678, 'parent\_id': '05c5f05af3db206ade590f467570f681', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cba8e4b95b03f6cb67d2945c1545d7a1', 'text': 'https://www.iso.org/', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 678, 'parent\_id': '05c5f05af3db206ade590f467570f681', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '807714d93f2e2d2985b98ca81d1818b0', 'text': 'https://csrc.nist.gov/', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 678, 'parent\_id': '05c5f05af3db206ade590f467570f681', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f595ed23acd702f18b3116049573a5b1', 'text': 'Part III: End to End 5G Security Architecture and Prioritizing Security Investments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 679, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a7e353cbab0f0cbd6646897abdd0506a', 'text': 'Chapter 10. Building Pragmatic End-to- End 5G Security Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 680, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f7693242f6db9c5cfa4f4f026649916e', 'text': 'After reading this chapter, you should have a better understanding of the following topics:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 680, 'parent\_id': 'a7e353cbab0f0cbd6646897abdd0506a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4716109411c67b5ee7d1b27f545fd044', 'text': '• Building a pragmatic security architecture for 5G networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 680, 'parent\_id': 'a7e353cbab0f0cbd6646897abdd0506a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '537075a49e20c1dd166950b177a7a411', 'text': '• Understanding key risks in the 5G ecosystem', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 680, 'parent\_id': 'a7e353cbab0f0cbd6646897abdd0506a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9c36188c28e7453667ac881269b65b5e', 'text': '• Key security controls and threat mitigations in the 5G ecosystem', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 680, 'parent\_id': 'a7e353cbab0f0cbd6646897abdd0506a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f248bd4a0dcb7683c56e7eab4e980bf6', 'text': '• Applying zero trust principles to secure 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 680, 'parent\_id': 'a7e353cbab0f0cbd6646897abdd0506a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '42e783f1bb12e4a9b57c3f566fa1c5b5', 'text': 'The previous chapters discussed the key security controls required per domain for different deployment types such as public, hybrid, and on-premises. We also saw the controls used to secure the 5G architectures, such as securing use cases based on standalone private 5G/5G non-public networks (NPN), Public Network Interface (PNI) NPN, service provider 5G networks, and network slice as a service (NSaaS). Understanding threats and mitigation techniques by each domain is very important if you want an enhanced and effective security posture. This chapter will take you through the considerations for building a pragmatic 5G security architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 680, 'parent\_id': 'a7e353cbab0f0cbd6646897abdd0506a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '183610b70c2046ede77650b729485bb7', 'text': 'This chapter will be of particular interest to the following individuals and teams from enterprise/5G service providers deploying 5GC as well as cybersecurity vendors planning product developments for 5G security use cases:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 680, 'parent\_id': 'a7e353cbab0f0cbd6646897abdd0506a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '47d1c8b99898ecdd9d4798bab9faa042', 'text': '• Government departments looking at security impacts of 5G deployment and looking at implementing security measures', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 680, 'parent\_id': 'a7e353cbab0f0cbd6646897abdd0506a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bd80ae1742f73efc9b0740ab5ad7c850', 'text': '• Management consultants advising governments and service providers on 5G security strategy', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 680, 'parent\_id': 'a7e353cbab0f0cbd6646897abdd0506a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '71a6a293a0aea8831c95d6e0e45fc8b2', 'text': '• CSO and CTO teams from service providers looking at securing 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 680, 'parent\_id': 'a7e353cbab0f0cbd6646897abdd0506a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e635e4457aa63a8795acd0226019a491', 'text': '• Enterprise teams deploying NPN/private 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 680, 'parent\_id': 'a7e353cbab0f0cbd6646897abdd0506a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3663a1dc816329a9d7150999e8985c8f', 'text': '• Security architects looking at securing 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 680, 'parent\_id': 'a7e353cbab0f0cbd6646897abdd0506a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd161eba7c2ee78a489a1de312520b213', 'text': '• Enterprise solution architects and enterprise security architects working with enterprises integrated with service provider 5G networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 681, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1906d2a36c260cdccc38763239ee7ecf', 'text': '• Cybersecurity vendor security architects looking to secure 5GC deployments for their customers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 681, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6052483d5e096faa11ea0366e857198c', 'text': '• Cybersecurity vendor product managers looking for use cases or features to enhance security products to cater for secure 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 681, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'de7a13616ce90884509755f1d3fb3bb1', 'text': "5G is not just a technology for providing better throughput to subscribers; it is the beginning of a technology revolution that will be the critical part of your country's infrastructure, allowing real-world use cases for government organizations, industries, enterprises, and citizens. 5G technology introduces a lot of flexibility in the way you can deploy the network as well as robust capabilities in creating and offering services to subscribers, which is unmatched by any of the previous technologies. Due to the many advantages that 5G provides, it will form the backbone of your country's economy and services provided by it. Once 5G is widely deployed, the networked government and private enterprises will be critically reliant on innovative new applications.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 681, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9db66625f5fed22b4f327c7a12373576', 'text': '5G is the first real cellular technology aimed at open integration with various third-party applications and systems to allow the realization of the use case. It is the first real technology where the network functions can be peeled away and deployed at the edge or at the enterprise premises to allow true low-latency use cases. 5G network slicing will play a critical role for use cases such as the smart factory, automotive, and the like. This also enables service providers to offer their network to the enterprise for better connectivity and to fulfill their use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 681, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '60c7c77af56f764d2185d374e3705cc1', 'text': "As you see due to the importance of 5G in the ecosystem, any attack on the 5G infrastructure could cripple a country's economy. What we really have to understand is that 5G is just the beginning. Upcoming technologies such as 6G, which is already in the works, will reuse the openness brought in by the 5G specifications and build on top of that to provide closer integration with other standards and frameworks to have a seamless functionality across multiple use cases. An example could be vehicle-to-everything (V2X), where practical realization of the use case would require integrations at least among vehicle-to- pedestrian (V2P), vehicle-to-infrastructure (V2I), vehicle-to-sensor (V2S), and vehicle-to-network (V2N).", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 681, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bbcfef94540ce37b197e5568576cc8d0', 'text': 'This chapter will take you through the key components and capabilities required by the security architecture to secure 5G deployments. The key topics covered in this chapter, such as the security architecture for open RAN (radio access network) and distributed RAN deployments, will be applicable to standalone private 5G/5G NPN networks as well as service provider networks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 682, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e24271a8b41bc96cf092376b624a8031', 'text': 'Foundations of 5G Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 682, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '74b3da1742dd336eedbfd26d1953b0ee', 'text': 'Building a security architecture for 5G will require you to have a completely different approach as compared to securing previous generations of cellular technologies due to the aforementioned applications of the 5G technology. Securing 5G deployments will require a holistic view of applying security. You will need to look at the 5G use cases your organization plans to implement and then build a security architecture which includes built-in security features and layers of security controls, ensuring that each of the use cases can be secured. This will require security architects to understand the use case first, which means involving the security teams early in the process and allowing the security principles to be integrated in the foundation of your 5G deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 682, 'parent\_id': 'e24271a8b41bc96cf092376b624a8031', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bc0968dfdcc00f20817685ebbf84e246', 'text': 'Having an end-to-end 5G security architecture includes protecting 5G network infrastructure, IT and OT network, and consumers of 5G services in any public or non-public deployment, as illustrated in the Figure 10-1. These different network areas or domains are usually separated by security zones and are catered by different teams within the organization. For example, a service provider will have separate teams catering for the 5G network infrastructure, such as radio planning and optimization, transport, back haul, and mobile packet core. A separate team is responsible for the IT and OT network infrastructure, usually called the network operations team. The managed services provided by the service provider is usually catered by a value added services team or a team under the Chief Revenue Officer (CRO).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 682, 'parent\_id': 'e24271a8b41bc96cf092376b624a8031', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '43cf3056e4ba4e8d93ca33f1697e070d', 'text': 'In legacy cellular networks, such as 4G, the 4G network infrastructure teams will not be much involved in the IT and OT network. Similarly, the IT teams within the organization will not be much involved in the cellular network operations.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 682, 'parent\_id': 'e24271a8b41bc96cf092376b624a8031', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '443e462883319bdb282978934153a2bd', 'text': 'However, for 5G, depending on the deployment mode (such as private 5G/standalone NPN 5G deployment), the teams responsible for IT and OT networks need closer interaction with the teams responsible for 5G infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 682, 'parent\_id': 'e24271a8b41bc96cf092376b624a8031', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b066d28fbc180e93fc96fc17af3e135', 'text': 'Figure 10-1 illustrates the key network domains to secure for public and non- public 5G deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 683, 'parent\_id': 'e24271a8b41bc96cf092376b624a8031', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '66ec713cf240b6e30a576f1ca333e77c', 'text': 'Securing 5G Securing IT& OT Network Components Components (IT network, lloT, PLC, SCADA network & (RAN, Packet Core, securing devices...) Public Cloud and on-premises deployment, Access & Aggregation, ...) Securing Consumers of 5G & Evolving Technologies (NSaa$S consumers...)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 683, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fdeb0efa54492b65eb1f8386d117ce16', 'text': 'Figure 10-1 Key Network Domains to Secure within Public and Non- Public 5G Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 683, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9e4725069929938854304773eb417d47', 'text': 'A typical service provider will have to cater for securing the three key domains shown in the Figure 10-1. For standalone NPN and PNI-NPN 5G deployments for industry verticals, apart from securing 5G network components, providing isolation between the IT and OT network components is important to ensure that attacks are not migrated from the IT part of the infrastructure to the OT', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 683, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f473e27830b2e407db76e6443ec12ebe', 'text': 'and IIoT network of the industry vertical. If deploying a NSaaS offering, you should ensure proper isolation between the slices and granular access control for users to prevent unauthorized access to customer slices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 684, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2bddbc9906fa87c9fd705d7c6b236041', 'text': 'Securing 5G and Evolving Network Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 684, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c4f08547a53e48d27ea3d037c4e79929', 'text': 'Securing 5G and evolving networks refers to securing the end-to-end components of the 5G infrastructure, which includes the RAN; access and aggregation, consisting of front-haul, mid-haul, and back-haul transport; multi- access edge (MEC) deployments in the public cloud and on-premises data centers; and Packet Core Network functions. it also includes the control Plane, User Plane, and Management Plane between the 5G network functions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 684, 'parent\_id': '2bddbc9906fa87c9fd705d7c6b236041', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '348bf8c3e3ebabcdb8e8db96e5335199', 'text': 'Securing IT and OT', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 684, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7813795679053ea426b2690766e0ab3a', 'text': 'In a typical network environment of any enterprise or service provider, you will be mainly dealing with the IT part of security. OT security is used primarily to protect and control critical infrastructures such as power stations, transportation networks, and smart city deployments. 5G use cases related to industrial Internet of Things (IIoT) requires integration between the IT and OT networks. Attempts to exfiltrate data, steal intellectual property, and disrupt operations are steadily increasing as more cyberattacks target critical infrastructure and industrial assets. Threat actors use weak security within IT networks to access and attack OT networks and exploit weak security implementation in OT networks to attack IT networks. These kinds of attacks are prevalent in critical infrastructure deployments such as oil and gas. To secure such critical infrastructure and industry vertical–related 5G deployments, you need to implement robust security controls on both the IT and OT networks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 684, 'parent\_id': '348bf8c3e3ebabcdb8e8db96e5335199', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4cdbbece0c8ebd5d8e04a793a84bead0', 'text': 'Securing Consumers of 5G and Evolving Technologies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 684, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4b12dd95f4be2efc8027ad9a5ed27b68', 'text': 'Service providers offering 5G services are referred to as communication service providers (CSPs). CSPs can also offer NSaaS to enterprise/industrial customers, which are referred to as communication service customers (CSCs). CSCs are categorized as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 684, 'parent\_id': '4cdbbece0c8ebd5d8e04a793a84bead0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '475906f47c39bd997053c22de2526071', 'text': '• Business-to-consumer (B2C) services: This category includes data (messaging, Internet and web surfing, and so on) and voice services (5G voice) to end customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 685, 'parent\_id': '4cdbbece0c8ebd5d8e04a793a84bead0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1a73aa16faf9cdb7e66d3a84b86d9828', 'text': '• Business-to-business (B2B) services: This category includes connectivity being provided to small, medium, and large enterprise businesses.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 685, 'parent\_id': '4cdbbece0c8ebd5d8e04a793a84bead0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9a4e24e2e5204f621590806461b79107', 'text': '• Business-to-home (B2H): This category includes home broadband, parental controls, and VPN services.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 685, 'parent\_id': '4cdbbece0c8ebd5d8e04a793a84bead0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '01414048f27b8dc71495d685c29c5fb9', 'text': '• Business-to-business-to-everything (B2B2X): This category includes services offered to other service providers, who in turn provide B2C/B2B/B2H to their end customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 685, 'parent\_id': '4cdbbece0c8ebd5d8e04a793a84bead0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '726695ed39074d41030cbc2036ed1e60', 'text': 'Key Tenets of 5G Security Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 685, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a9e5bb98888b9d76c1cef9310b18bda', 'text': 'Figure 10-2 illustrates the key tenets of 5G security architecture.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 685, 'parent\_id': '726695ed39074d41030cbc2036ed1e60', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '19b4b30ca229303b31e8a663ce489b0d', 'text': 'Secure infra Supply Chain and inter- network security (HW &SW) Connectivity Granular Device & User Access controls based on Enhanced zero trust visibility & principles Monitoring 5G & evolving Secure technologies Interoperability - Private 5G, Slice Level National NW & Security - Intra & Inter- Inter-National NW Slice Vulnerability Application Management & level security Forensics', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 686, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d60f0775047e85a5113f866b8970e0c', 'text': 'Figure 10-2 Key Tenets of 5G Security Architecture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 686, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '30ec1b14b73233c0e52f092db17630b8', 'text': 'Whereas each of the chapters in Part II, “Securing 5G Architectures, Deployment Modes, and Use Cases,” went into detail on the key security tenets for the respective domains, as shown in Figure 10-2, the sections that follow look at these tenets from the perspective of an end-to-end security architecture for securing your 5G network along with its use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 687, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'text': 'Supply Chain Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 687, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'be355f746dce30a0281ab5648dfad721', 'text': 'The significant risks of supply chain threats arise from nation-state actors who aggressively target service provider and public sector networks to exfiltrate sensitive information, modify certain parameters to compromise critical infrastructure, destroy information, or cause an outage in order to cripple a country or the private/public sector. Until the 2010s and early 2020s, supply chain attacks were related mainly to hardware and required a certain amount of sabotage, including coercing the hardware engineers and designers in printed circuit board (PCB) design and manufacturing teams to change the PCB schematic or modify it to include an extra track to include a component for sniffing purposes. Once the design team was infiltrated, it became difficult to identify any anomalies in the design because the quality team had the modified schematic. This can still be carried out and is actually difficult to detect because any given hardware related to telecom infrastructure has a complex PCB design. This is also difficult to detect during functional testing, as the components can remain quiet unless triggered remotely once deployed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 687, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d366c9851896a218620acf5713549a4', 'text': 'This risk has been present for ages in one form or another. So what makes it important now?', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 687, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '406dfe0f0785cede842c299e8b4932ff', 'text': "If you take a step back you will see that many of the communication companies providing voice and data services using legacy technologies had their critical network functions and devices air-gapped, meaning they were isolated and didn't have any interactions with the Internet. Of course, we had the SS7, GPRS Tunneling Protocol (GTP), and Diameter-based threats, but those fall under network and protocol security, which we can cater to with specialized firewalls.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 687, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8276a1d0df7b19722a5c49fc3b452885', 'text': 'Beginning with 5G, the entire ecosystem is based on openness. Various models such as NSaaS allow service providers to logically peel away parts of their network and offer them to industries, government sectors, and enterprises. Other models such as Cloud RAN/Open RAN/Virtual RAN, private 5G/NPN, and PNI-NPN can be used by any of the industry verticals to create their own', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 687, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2b7339f8be461b04870ea41feac020d2', 'text': '5G network using their own spectrum or a spectrum leased from service providers who own parts of the spectrum.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 688, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6c1a45ff3ada0d1d580d26f48c088701', 'text': "As the nation's entire ecosystem is run by 5G and other evolving architectures, robust security processes should be planned by the national cybersecurity agencies to prevent disruption to the country's economy. The security agencies should be looking at the virtualization scenario as a priority. Virtualization, although not new, has expansive use in telecom via the use of Cloud-Native Functions (CNFs), which have emerged only during the 5G evolution. The entire 5G network functions will now be based on CNFs, which use open- source software to create 5G network functions, which can then be deployed as a virtual machine (VM) or a container on any hypervisor on the premises or any multistack public cloud infrastructure. As an example, any government or industry vertical can now deploy its own 5G network with all the 5G network functions on the public cloud.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 688, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e9ca0c50a450c441a3dc16d23fbbac2c', 'text': 'Here are some of the security processes that can be followed by the service provider, government entity, or any industry vertical deploying 5G:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 688, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '57a7faa548ea13ff5b95e3090bce3545', 'text': '• The cybersecurity agency of the country should lay down the key security controls required for the deployment of 5G, other than the security controls stated as mandatory by 3GPP specifications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 688, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '01230a82987bb4173eb9eac260582adc', 'text': '• The cybersecurity agency of the country should have an incident response (IR) team specifically for the national critical infrastructures and key industry verticals. Of course the industry verticals and critical infrastructure providers will have their own security operations center (SOC) and IR, but an overlay team is important to ensure the right skills are in place during a drastic nation-state attack.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 688, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5e860f145144413da83a302c2e125f2b', 'text': '• Test centers should be shared for different countries, reducing bottlenecks for service providers in deploying 5G networks. Instead of having separate testing centers of equipment for each and every country in Europe, there should be three to four test centers led by a joint effort for specific testing to certify the network functions and devices. This would improve the rate at which the NFs and telecom service equipment could be tested.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 688, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4240d75dc738f491261674807b1ba9e1', 'text': '• The cybersecurity agency of the country should provide services to audit the 5G network for nation-state-specific risk vectors.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 688, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9190cf780c3a0ce69fc2a3f114a39405', 'text': '• Most software depends on third-party components (libraries, executables, or source code), but there is very little visibility into this software supply', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 688, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'face954a47794ffcc8bbdf37c06ce883', 'text': 'chain. It is common for software to contain numerous third-party components that have not been sufficiently identified or recorded. Methods such as software bill of materials (SBOM), which is a formal record containing the details and supply chain relationships of various components used in building software, will help you identify the “ingredients” of software installed on any system or device. This can save hundreds of hours in the risk analysis, vulnerability management, and remediation processes. The SBOM initiative is a National Telecommunications and Information Administration (NTIA) multistakeholder process on software component transparency.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 689, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2e3b75afef6f415fbd0adaf83cb00427', 'text': '• 5G deployments should have a solid network and application monitoring layer with tight integration capabilities with critical telecom service equipment and applications. This allows early detection of any attacks on the critical infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 689, 'parent\_id': 'c58e8558b155fa63149bbb9f79bd19d7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a1c3f0f01f358076cd7f98855df6a5cf', 'text': 'Securing User and Device Access Using Zero-Trust Principles', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 689, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ef8e561cd38c972f4a76c1e6247a77ce', 'text': "Traditional networks are based on defined perimeters, where most of the mobile packet core functions are centralized. The evolving mobile packet core architectures such as 4G Control Plane and User Plane Separation (CUPS) and 5GC using MEC create software-defined perimeters. The 5G core is based on a cloud-native architecture that allows 5G core network functions to be deployed as a microservice in a private data center of the service provider or in a public cloud such as Amazon, Azure, Google Cloud, and so on. Multiple vendors will supply Network Function Virtualization Infrastructure (NFVI) components and Virtualized Network Functions (VNFs). In addition, many contractors and sub- contractors will require access to the network for support, configuration, and deployment purposes. Many of the interfaces in the 5G core rely on web-based communications, including the Representational State Transfer–based API, which doesn't have any predefined security methods, so developers need to define their own. The previously mentioned threat vectors and threat actors in 5G drive a requirement of having a robust security foundation while deploying 5G networks.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 689, 'parent\_id': 'a1c3f0f01f358076cd7f98855df6a5cf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aa678c46ede0076629eb5b4e5ad4e7fe', 'text': 'Zero trust for 5G consists of multiple layers of security, establishing trust in user identity, enhanced end-to-end visibility, and the trustworthiness of the user device accessing the data control network (DCN). Enforcement using risk-', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 689, 'parent\_id': 'a1c3f0f01f358076cd7f98855df6a5cf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1f2c3b8276033de95073a53a0fa31d1a', 'text': 'based and adaptive access policies while enabling secure connections to devices and applications can then be undertaken. Figure 10-3 illustrates the main models within zero-trust security for 5G deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'parent\_id': 'a1c3f0f01f358076cd7f98855df6a5cf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '0c17f0bb56459aca8b2f46d36dbcd8fd', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '1bc6d81ecbfa4d2c7b6cba1ca31a6026', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '622d5e87864bf222342ab77eb994b47e', 'text': '¢85', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4e56035b9088db8706f434ea45c6bd0f', 'text': 'Zero trust workforces', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'cf1dde543aa71070cf0399d75a5fafc0', 'text': 'Zerotrust data', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '35123c71d62dfb82d1a5529a0e047601', 'text': 'Zero trust workloads & servers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'parent\_id': 'cf1dde543aa71070cf0399d75a5fafc0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '93edf6db1ab9c33921d22cc1d354acc8', 'text': 'Authenticate users and continuously monitor and govern their access and privileges. Secure and verify users, user access and privileges as they interact with the Mobile Packet Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'parent\_id': 'cf1dde543aa71070cf0399d75a5fafc0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0899ef23efa54cebd9beafecd649f6b6', 'text': 'Secure and manage data, have enhanced visibilty on the packet flows in the Mobile Packet Core and have visibiity and conrol mechanisms to prevent data exfitration of sensitive data', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'parent\_id': 'cf1dde543aa71070cf0399d75a5fafc0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f4dc29971d00f95ac3d0c66749fd7bc8', 'text': "Enforce controls on the end to end stack, especially securing the hardware connections between VM's, containers and AP! calls in the Mobile Packet Core", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'parent\_id': 'cf1dde543aa71070cf0399d75a5fafc0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a5a62193352030bca0e019c8b8d8f434', 'text': 'Figure 10-3 Main Zero-Trust Security Models for 5G Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd450e552772d1bfc2e134188e852fe89', 'text': 'Risk-based and adaptive access policies provide a control mechanism and the security policies for the users and devices. Some controls are taken proactively, while others are applied after an attack takes place. There are two types of attacks:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '462b9ba098420c6658a39ac91225f6cf', 'text': '• Zero-day attacks are threats that are previously unknown.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ac3f1106e98c1a997ffecff61f0a020a', 'text': '• Day-one attacks are threats that have been communicated by the vendor but have not necessarily been patched in the production environment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aba308c39d99a913c3ab1ad4d4edcfae', 'text': 'Typically, deviations in known-good behavior of the carrier cloud and the applications that request service and state from it are identified by the security controller, and then some action is taken to mitigate the attack or to gain additional visibility. An action is then taken to properly identify the miscreant and mitigate the risk. Day-one or n-day attacks are attacks where publicly acknowledged vulnerabilities are leveraged before the vendor releases the security patch or before the customer has applied the security patch to mitigate', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 690, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '670f62be71e4f8ed2d6ba7bc75ba2526', 'text': 'the vulnerability. These attacks can be reduced by ensuring that the latest patch is applied to minimize the damage caused by the vulnerability exposure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 691, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0340a8dde88e2d26fdffcc9bdbdfd91b', 'text': 'One of the critical parts of your 5G network is the data control network (DCN), which provides management access to the packet core elements and is predominantly used by network management systems (NMSs) as well as third- party vendors for troubleshooting access and for internal command-line access for configuration and troubleshooting. Typically, the DCN provides the following:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 691, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ffbb499b0d845875aa82ff2d14eb7fe7', 'text': '• VPN remote access for third-party vendor troubleshooting and for internal remote support', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 691, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '47f70fb318d941a6543a3085a92a4fff', 'text': '• “Gray” management Virtual Routing and Forwarding (VRF) for transport across MPLS cores', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 691, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '794d612fb0e3d657c86460b5a262b3ba', 'text': '• Routed and switched network infrastructure for DCN traffic (for example, logging, configuration, and performance management)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 691, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '26591ac1e8d4a680c8ead8a5882d9f4f', 'text': '• A proxy or “jump host” to break external communication and provide proxied access', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 691, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '49c5869d10c508d7d62d9cf32fb48adb', 'text': '• Logging and reporting of user access and commands issued by each user', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 691, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8225945d4ba2b9d9588d10795dbf98f3', 'text': '• Out-of-band access to lights-out management (LOM) and console ports (terminal server access)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 691, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c7bec08118f387fa2f051c77bf12f672', 'text': 'Vendor access into the DCN to provide support assistance is a normal requirement; however, credential reuse (sharing a single password for multiple people within the vendor) and the potential for staff churn are both possible risks that allow unauthorized access to devices. This can be mitigated through the use of a VPN concentrator in combination with multifactor authentication (MFA) technology.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 691, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '323ba3c21f103c3df465e7d2d661bffb', 'text': 'Once a specific vendor has authenticated and is allowed onto the DCN, it is not uncommon that they would have unfettered access to all the devices connected to the network, which includes the management access layer of other vendors. In a zero-trust methodology, we would want to limit vendor A to accessing only the elements they need to support, while also limiting the protocols allowed on that interface, as shown in Figure 10-4.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 691, 'parent\_id': 'a5a62193352030bca0e019c8b8d8f434', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a3f38f69d8fd1e34763ec19bd8147ee9', 'text': 'Vendor Vendor 1 1] Equipment 1 Vendor Vendor 2 Equipment2 1] om- Vendor Vendor 3 Equipment 3 v 1]', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 692, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '690e7736e632f14ec6ee3115aef60d4a', 'text': 'Figure 10-4 Applying Zero Trust principles for Vendor Specific Access', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 692, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '666331354db790dabc4f2fe73b8e6a4e', 'text': "Visibility plays a key part in understanding security and can be enabled on the DCN through extensive logging of activity via RADIUS and TACACS+, with a focus on ensuring that log data is able to be stored for a long-enough period for forensic investigation purposes. Understanding network traffic profiles and potential data exfiltration can be achieved through an anomaly detection engine, which can automatically baseline normal traffic and identify data being exfiltrated. Figure 10-5 shows an example of multiple remote users accessing the service provider's network resources.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 692, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '333ce81c915b1e08e7d16d450eb35238', 'text': 'Contractors [} | [} Y L Employees [ u] l; Sub-Contractors M Viendors °l IoI < Cloud Services / JJ Applications ¢', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 693, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '037efb9de0d4e3b19a0ff20c6e9c68ef', 'text': '~ / — R 1 DU, CU l @ 1 CU, UPF 1 56C, EPC | - | VRAN Apps i MEC Apps | Packet Core Apps P . ﬁ S i E L E \\eesseneens! |n Fronthaul WAN oem ((A)) J @ Midhaul @ Backhaul aEn Far Edge DC Edge DC Central DC S - Off-Prem S L ——', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 693, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '25812647f8b1eea4ff82b23c198dd2c7', 'text': 'Figure 10-5 Applying Zero-Trust Principles for 5G Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 693, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e92eff7c55d4d80151ff0377a4fa330d', 'text': 'As shown in Figure 10-5, the network has multiple personnel (employees, vendors, contractors, and sub-contractors) accessing the infrastructure, which includes multivendor NFVI, multivendor VNFs, and containers for various provisioning, operational, and maintenance purposes. To prevent malicious actions intentionally and unintentionally in 5G networks, there are three steps', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 693, 'parent\_id': '25812647f8b1eea4ff82b23c198dd2c7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dd78e3a773f550280e22eaf5dfa77f53', 'text': 'through which the operator could deploy a zero-trust security architecture in 5G networks, which are listed next and illustrated in Figure 10-6:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 694, 'parent\_id': '25812647f8b1eea4ff82b23c198dd2c7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '63d86dae7d79bf02e10fb72dac44f24b', 'text': 'Step 1 Implement a VPN layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 694, 'parent\_id': '25812647f8b1eea4ff82b23c198dd2c7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '26cce76ba4835f6ebcaf88ff759bcdf3', 'text': 'Step 2 Implement multifactor authentication (MFA) and segmentation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 694, 'parent\_id': '25812647f8b1eea4ff82b23c198dd2c7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8df40b63c04268ee3324ffeac018b0e1', 'text': 'Step 3 Implement an enhanced visibility and threat mitigation layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 694, 'parent\_id': '25812647f8b1eea4ff82b23c198dd2c7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '2572c548ecc1756cdfd67d9ba3992c10', 'text': 'u| | 8] M Stept: Securing L Remote Access Cloud Serviees connections using LR & Applications PN Step 3: Enhanced Visibity and Threat d 4 mitigation User+Device vy Step 2: Mult-Factor Authentication and Vi Segmentation Network & User Access & Logs Cloud H Telemelry (cess Policy >, , — ou,CU 1 56C, EPC CU, UPF = VRAN Apps MEC Apps 1 Packet Core Apps é : T ﬁ \\8— &, g \\, i |n ! e e e 2 nem WAN L[] ] Michaul @ Backhaul s ). Far Edge DC Edge DC Central DC O — = Off-Prem e R ————', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 694, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7fef033817b3cb9b4d7e6852dfa2355c', 'text': 'Figure 10-6 Applying Enhanced Visibility and Granular Access Controls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 694, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '862fb39742581fa03527fc834f6c09cc', 'text': 'The three steps in having a zero-trust access layer for the 5G network are further discussed next:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 695, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '34f162405684c170be8eecde10a6c505', 'text': "Step 1 VPN layer: As the first step, a VPN could be used for any external access to the service provider's DCN. VPNs use the IPsec protocol suite for packet encryption, authentication, and nonrepudiation. VPN includes protocols for establishing mutual authentication between agents at the beginning of a session as well as negotiation of cryptographic keys to use during the session. It can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol Security (IPsec) uses cryptographic security services to protect communications over IP networks and also supports network-level peer authentication, data- origin authentication, data integrity, data confidentiality (encryption), and replay protection.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 695, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '51039cb097a289cf6066c3011dadd3b6', 'text': "Step 2 MFA and segmentation layer: The next step is to deploy the policy control and enforcement layer along with the multifactor authentication (MFA) layer and segmentation using a Network Access Control (NAC) solution. The user authenticates to NAC, and the device is verified to make sure it is authorized for access to the requested part of the network. The switch or wireless LAN controller (WLC) tags the traffic. As an example, mechanisms such as Security Group Tag (SGT) can be used to tag the traffic. Using an SGT, you will be able to group each vendor's access and control access to network and application resources on a granular level. Then the policy is enforced on the data center firewall with a firewall that allows EPC and 5G core resources (hardware and VNFs) access only to those devices and users that are authorized; all other devices and users are denied access. SGTs are applied to authenticated users to explicitly allow access for authorized users by using security group access control. Using this mechanism, you can provide and enforce access security policies based on user, device, and application risk as well as verify the identity of all users. This integrated solution provides security admins with the ability to enforce consistent user- and device-based policy for VPN access and thereby reduce the risk of data breaches while meeting compliance requirements.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 695, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b4b3626166e7d0146e4f20648dfe9329', 'text': 'Step 3 Enhanced visibility and threat mitigation layer: The enhanced visibility and anomaly detection layer will require integration with the NAC layer to obtain key information, including MAC address, IP address, last active time, user name, security group, VLAN, domain name, interface device IP, and interface device port ID. These key pieces of information, coupled with network visibility using the network and application telemetry, allow you to provide key insights into endpoint behavior and identity as well as to indicate anomalous behavior. However, not everything unusual is malicious; therefore, enhanced visibility solutions, along with ML and AI integrations, can quickly and with high confidence correlate anomalies to threats such as C&C attacks, ransomware, DDoS attacks, illicit crypto mining, unknown malware, as well as insider threats. In addition to this, the enhanced visibility layer should be able to analyze encrypted traffic without decrypting the encrypted traffic. This is particularly relevant when the level of encrypted traffic is used for API communications between 5G and external networks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 696, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e15e0c419f7a372538a25504bf2f7c4e', 'text': 'These three steps can help ensure that you authenticate users and continuously monitor and govern their access and privileges. It also provides a method to secure and verify users, user access, and user privileges as they interact with the 5G network, thereby mitigating malicious actions and intent.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 696, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '62fc0f5a19d9454f572c66ad274279c3', 'text': 'Your network will encompass a diverse range of technologies—from legacy signaling protocols to the latest distributed, virtualized environments, including multivendor NFV and multivendor Virtual Network Functions (VNFs) based on virtual machines and containers. This broad attack surface creates gaps in the security posture that can be addressed through the use of trusted platforms, enhanced anomaly detection, granular control on workloads, and limiting communication in line with the zero-trust methodology.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 696, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0580f11a8e04f6ae8f164ad6b1be93f3', 'text': 'Table 10-1 provides a checklist for granular access control on DCNs mainly used for Day 0 and Day 1 configuration, operations, and maintenance', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 696, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'd7614808a4c7c27bde892873d0bf4f4e', 'text': 'Recommended Security Controls Does This Security Solution/Feature Control/Capability Used Exist in Your Network? (Y/N) Remote user VPN Multifactor authentication Device profiling Microsegmentation Endpoint protection Granular visibility and immediate quarantine DNS security for users and devices lIoT device authentication and authorization', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Recommended Security Controls</th><th>Does This Security Control/Capability Exist in Your Network? (Y/N)</th><th>| Solution/Feature Used</th></tr></thead><tbody><tr><td colspan="3">Remote user VPN</td></tr><tr><td colspan="3">Multifactor authentication</td></tr><tr><td colspan="3">Device profiling</td></tr><tr><td colspan="3">Microsegmentation</td></tr><tr><td colspan="3">Endpoint protection</td></tr><tr><td colspan="3">Granular visibility and immediate quarantine</td></tr><tr><td colspan="3">DNS security for users and devices</td></tr><tr><td>lIoT device authentication and authorization</td><td></td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 697, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9637fa5ed5490c71c7ba59c4f2428155', 'text': 'Table 10-1 Security Control Checklist for Granular Access Control', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 697, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a61f7dad71093e3b5bafa97caafee974', 'text': 'Secure Intra/Inter-Network Connectivity', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 697, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '178fb8fa5c9d79b9e3ade07050510d06', 'text': 'Secure intra/inter-network connectivity caters to securing the following components of 5G:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 697, 'parent\_id': 'a61f7dad71093e3b5bafa97caafee974', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ab28dd1ca3d4fef5f1d87101ae40bd2f', 'text': '• Access and aggregation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 697, 'parent\_id': 'a61f7dad71093e3b5bafa97caafee974', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e40ddf92251e238e37c8e5fecbeb66c3', 'text': '• DDoS protection', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 697, 'parent\_id': 'a61f7dad71093e3b5bafa97caafee974', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9fba56fb5b5b6bc1c2ae6098d576b41d', 'text': '• API security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 697, 'parent\_id': 'a61f7dad71093e3b5bafa97caafee974', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd29b198fc66058f14afd4fb83ee495a6', 'text': '• Infrastructure security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 697, 'parent\_id': 'a61f7dad71093e3b5bafa97caafee974', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4cdfb6d52266398030059d464cdba3f4', 'text': '5G makes it possible for the network functions to be deployed in on-premises, public cloud, and hybrid modes. 5G use cases such as smart factories with ultra-reliable low-latency communication (URLLC) can be realized using', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 697, 'parent\_id': 'a61f7dad71093e3b5bafa97caafee974', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7ad192eb4e4f78ac14059f8b10d21d21', 'text': 'various architectures such as Open RAN or Distributed RAN, using multiple 5G network deployment methods such as standalone NPN/private 5G, PNI- NPN, or by reusing the service provider infrastructure using network slicing and deploying NSaaS models. Moreover, all these different deployment modes require integration with an external IT and OT layer, SDN, orchestration layer, and third-party application layer. All this flexibility and openness makes 5G different from its predecessor, but also requires careful planning of security controls to ensure that the network connections are secure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 698, 'parent\_id': 'a61f7dad71093e3b5bafa97caafee974', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '347fc1d98c623f367bfb26bb9dd385c2', 'text': 'Although IoT might not be planned in the first year of deployment in service providers, IoT is one of the primary use cases for industry verticals such as smart manufacturing that are planning to use NPN and PNI-NPN 5G deployments. Threat surfaces such as weak built-in security of the network devices and peer-to-peer communication by use cases such as vehicle-to- everything (V2X) bring in new risk vectors.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 698, 'parent\_id': 'a61f7dad71093e3b5bafa97caafee974', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b3c439092c63fa0a1d98f966332dd5cd', 'text': 'The fulfilment of NPN and PNI NPN 5G use cases rely heavily on non-3GPP- based communications and traversing insecure public networks, which are prone to man-in-the-middle (MitM) attacks. The required security controls and capabilities would depend on the deployment model being used for 5G and the use case being catered by the deployed 5G network. Figure 10-7 illustrates securing the connectivity of 5G packet core network using inherent methods such as using SEPP and SCP introduced by 3GPP and other overlay security mechanisms such as API gateway (GW) and web application firewall (WAF).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 698, 'parent\_id': 'a61f7dad71093e3b5bafa97caafee974', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '4d1c9bcc80c7cc6193761cce1eaa651c', 'text': 'APIGW | WAF to mitigate attacks exploting API vulnerabilties miLS Analyzing encrypted traffic for malware without decrypting the trafic 5G Packet Core CNF I SR () NS SF NRF o ; Nud e e e —— — Nnss| | e ———— Norf [[| 7 Nocf]| Naf I Nnef | | E Nam | Naus| == ul é - r e = Signaling exchange between service HPLMN | VPLMN Use SCP (optional 3GPP) for creating NF <> NF communication mapping and high- providers (roaming networks) - using API level global access list efc', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 699, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'cf84f3c7c96f9c79b8c42b16468d22cc', 'text': 'Figure 10-7 Securing the API Using Multilayered Security Controls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 699, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2dc2d04069391d70e5e654799563c041', 'text': 'Figure 10-8 illustrates securing the connectivity of various interfaces in a 5G deployment using SecGW and TLS mechanisms.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 699, 'parent\_id': 'cf84f3c7c96f9c79b8c42b16468d22cc', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'b774ef7bec35720aad0c101a4b033eba', 'text': 'DU, CU,5GC UP & CP, MEC Appln SecGW only for non-AP! traffic AAU | APIGW / WAF, SecGW, Anti-DDoS (¢ amm———— o= mo = 5GC, EPC ou,Cu RU, DU Sec- 2 E \\?J, UPF Sec- |y | — Sec =88 ———ow oW g GW / Mid Haul Back Haul : Front Haul (FH) (MH) (BH) PKI', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 700, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ca65ba9a252149d8842448c217ee3095', 'text': 'Figure 10-8 Securing Intra- and Inter-Network Connectivity', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 700, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c9aa624e3bd2a027e4bac5901412c5ae', 'text': 'Figure 10-8 shows using a security gateway (SecGW) to provide encryption and authentication of the nodes deployed between the front haul (FH), mid haul (MH), back haul (BH) and the public deployed 5G 3GPP components.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 700, 'parent\_id': 'ca65ba9a252149d8842448c217ee3095', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7871578cf61873ec5595401f4b3d356d', 'text': 'Web application firewalls (WAFs) and API gateways are the two major inline security tools for API protection. While API gateways do usually offer authentication and authorization features, the HTTP and OWASP Top 10 protection offerings are either limited or absent. To protect API-based communications, a WAF can be used to ensure APIs are secured. Any Internet- facing APIs or APIs external to the on-premises 5G packet core components', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 700, 'parent\_id': 'ca65ba9a252149d8842448c217ee3095', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ce44589eb20d1294f02818061f70d2fa', 'text': 'should be secured by using Transport Layer Security (TLS) mechanisms and an API gateway or WAF to mitigate API-related risks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 701, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4e32fe30bcc002b13eb05226cf91daf2', 'text': 'The internal communication between the 5G NFs should be authenticated and authorized. This could be catered for by using mechanisms like OAuth 2.0, which uses authorization tokens to prove an identity between NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 701, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '99b0758f21c77bcd9759a6ae325c487b', 'text': 'For internetwork connectivity in use cases such as PNI-NPN, the interfaces between the enterprise, and the service provider should be secured. Depending on the deployment model, the internetwork communication could be just an API, which can be secured using TLS or the control and user planes and might require both TLS for securing the API and IPsec to secure the non-API requests.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 701, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7ce2231f7da7bb9ce10451e071fce4e0', 'text': 'For use cases such as NSaaS, API communication should be secured, and granular user authentication and authorization should be implemented.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 701, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5cc8e723d50d56585d1d010986b18874', 'text': 'Table 10-2 provides a checklist for securing access and aggregation for 5G deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 701, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '349564d294dcb94cda346415b81189ae', 'text': 'Recommended Security Controls Does This Security Solution/Feature Control/Capability Used Exist in Your Network? (Y/N) Hardened software and hardware Encryption in back haul/xHaul Authentication for nodes in back haul/xHaul Visibility on nodes in back haul/xHaul (control plane monitoring) DDoS protection (from devices within the network and from devices outside the network) Spectrum scanners PKl infra API security for programable access and aggregation routers Secure Zero-Touch Provisioning server for access and aggregation equipment and devices', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Recommended Security Controls</th><th>Does This Security Control/Capability Exist in Your Network? (Y/N)</th><th>Solution/Feature Used</th></tr></thead><tbody><tr><td colspan="3">Hardened software and hardware</td></tr><tr><td colspan="3">Encryption in back haul/xHaul</td></tr><tr><td colspan="3">Authentication for nodes in back haul/xHaul</td></tr><tr><td colspan="3">Visibility on nodes in back haul/xHaul (control plane monitoring)</td></tr><tr><td colspan="3">DDoS protection (from devices within the network and from devices outside the network)</td></tr><tr><td colspan="3">Spectrum scanners</td></tr><tr><td colspan="3">PKl infra</td></tr><tr><td colspan="3">API security for programable access and aggregation routers</td></tr><tr><td>Secure Zero-Touch Provisioning server for access and aggregation equipment and devices</td><td></td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 702, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f949038b7527a0fd9bc3eaccea3a847a', 'text': 'Table 10-2 Security Control Checklist for Access and Aggregation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 702, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f80ebf102f73ec0203837ac5068e8523', 'text': 'In 5G, new formats of user equipment, including low-cost insecure IoT devices, could introduce new kinds of vulnerabilities that might be exploited to target user data confidentiality and integrity. Abuses on hardware and software implementations on the user equipment (UE) side can stem from installation of malicious components that might compromise confidentiality and the integrity of subscriber profile data. The threat includes the theft of user credentials, brute forcing of user accounts, password cracking, masking the user identity, and impairment of IoT grouping authentication as techniques used by threat actors to abuse the 5G authentication systems. Table 10-3 describes the security controls and capabilities to secure the IoT/IIoT deployment phase.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 703, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '1685010fb4ae4560349e7c5d303df2d7', 'text': 'Recommended Security Controls Does This Security Solution/Feature Control/Capability Used Exist in Your Network? (Y/N) DNS protection for loT devices PKI config for loT devices API gateway API visibility Encrypted traffic analysis for control plane DDoS protection from loT devices and external and internal DDoS attacks loT application protection (security policy enforcement per loT application) Web application firewall, including rate limiting Authentication and authorization of lIoT devices Anomaly detection and monitoring of IoT/IIoT network (including OT) Segmentation between IT & [1oT/OT network', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Recommended Security Controls</th><th>Does This Security Control/Capability Exist in Your Network? (Y/N)</th><th>Solution/Feature Used</th></tr></thead><tbody><tr><td colspan="3">DNS protection for loT devices</td></tr><tr><td colspan="3">PKI config for loT devices</td></tr><tr><td colspan="3">API gateway</td></tr><tr><td colspan="3">APl visibility</td></tr><tr><td colspan="3">Encrypted traffic analysis for control plane</td></tr><tr><td colspan="3">DDoS protection from loT devices and external and internal DDoS attacks</td></tr><tr><td colspan="3">loT application protection (security policy enforcement per loT application)</td></tr><tr><td colspan="3">Web application firewall, including rate limiting</td></tr><tr><td colspan="3">Authentication and authorization of lIoT devices</td></tr><tr><td colspan="3">Anomaly detection and monitoring of IoT/IIoT network (including OT)</td></tr><tr><td>Segmentation between IT &amp; IIoT/OT network</td><td></td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 704, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'abb419b01e944ddc695dbf7048fca589', 'text': 'Table 10-3 Security Control Checklist for IoT/IIoT Deployment, API Security, and DDoS Protection', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 704, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '17cec0c6cbd7564bced1cb1fcd3cfd98', 'text': 'Furthermore, you also need security controls to discover network traffic with application-level insight, to classify and manage application sessions such as', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 704, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a60e01e8c610ce3e451e70e7d4063208', 'text': 'web browsing, multimedia streaming, and peer-to-peer applications, to monitor application usages and anomalies, and to build reporting for capacity planning and compliance. Table 10-4 provides a checklist for these security controls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 705, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '51dc7d32d21ef40960790e301f0ad1df', 'text': 'Solution/Feature Recommended Security Controls Does This Security Control/Capability Used Exist in Your Network? (Y/N) Application-aware firewalling Anti-malware using sandboxing for infrastructure users SSL decryption and inspection Rapid threat containment Application visibility and control Macro and microsegmentation', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Recommended Security Controls</th><th>Does This Security Control/Capability Exist in Your Network? (Y/N)</th><th>| Solution/Feature | Used</th></tr></thead><tbody><tr><td colspan="3">Application-aware firewalling</td></tr><tr><td colspan="3">Anti-malware using sandboxing for infrastructure users</td></tr><tr><td colspan="3">SSL decryption and inspection</td></tr><tr><td colspan="3">Rapid threat containment</td></tr><tr><td colspan="3">Application visibility and control</td></tr><tr><td>Macro and microsegmentation</td><td></td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 705, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0b65eb42bc7c3454f6fe0692958e2686', 'text': 'Table 10-4 Security Control Checklist for Infrastructure Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 705, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'text': 'Application-Level Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 705, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '47d96d5c68248ba17b68b5d21cae88ae', 'text': '5G deployment is based on the CNF deployment model, which is actually a software implementation of a 5G Network Function (NF) using open source software instead of legacy deployments, which traditionally would be performed by a physical device. The CNF deployments could be based on VMs and/or containers that communicate with other 3GPP and non-3GPP NFs via standardized RESTful APIs. CNF deployment models bring in advantages such as being independent of the guest operating system (when deployed as containers) and the ability to scale with a small performance footprint. Service discovery and orchestration add to these advantages by bringing enhanced resiliency to node failures.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 705, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '378cc418de75c1af0c618267c466c0c6', 'text': 'While adherence to CNF deployment does bring the aforementioned advantages in 5G deployment, you should allot for new risk vectors such as vulnerabilities from guest hardware and operating systems (OSs) as well as vulnerabilities in the open source software components used to build 5G 3GPP and non-3GPP NFs. 5G cloud-native architecture will bring in the need for industries to adopt a new development framework and move quickly to a cloud-native environment with virtualization, automated deployment, instantiations, and upgrades, by leveraging open source technology and software stacks. This affects not only new 5G services planned to be delivered by service providers, but also represents new ways for enterprise and industry verticals to consume those services. The four pillars of cloud native architecture—DevOps, microservices, containers, and continuous delivery— are all in play as we leverage open source technology. Cloud-native architecture splits the applications and 5G Network Functions (NFs) into individual microservices and focuses on decomposition to allow distributed deployments when it brings value. Some of the key security process, controls, and capabilities are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 706, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3ac71a7b96d9f020da3faff83b9afa2f', 'text': '• Application-first security methodology: Accelerated application development and deployment for 5G networks will require DevOps to bring together software development and operations to shorten development cycles, allow organizations to be agile, and maintain the pace of innovation while taking advantage of 5G cloud-native architecture. However, existing DevOps practices used to develop and deploy software in operational environments can be implemented without consideration of security, leading to reduced efficacy and effectiveness of point-in-time threat modeling of the 5G network. This has shifted the industry mindset from infrastructure-first to application-first security. Processes such as development security and operations (DevSecOps) bakes in security at every step of software design. Development, testing, and quality enable the development of secure software with the speed of DevOps. Instead of depending on various inspection algorithms to identify the security gaps within the code, DevSecOps aims to have secure software earlier in the development process. DevSecOps helps ensure that security is addressed as part of all DevOps practices by integrating security practices and automatically generating security and compliance artifacts throughout the process. DevSecOps practice needs to be implemented by 5G vendors and service providers to ensure secure deployment of 5G cloud-native network functions. Both the vendors and', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 706, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'db9498c2991bedc971ea7c8a00143772', 'text': "service providers will benefit by following the DevSecOps methodology. For vendors, following the DevSecOps methodology ensures reduced vulnerabilities, malicious code, and other security issues in the hardware and software stack being deployed in service providers' 5G critical infrastructure, without slowing code production and releases. For service providers, implementing DevSecOps methodologies will help address security issues such as any vulnerabilities and malicious code before its deployed on the production node, thus improving security efficacy for the 5G network. If you have a software development team to cater for 5G MEC applications, then following the DevSecOps methodology will help you addresses security issues as soon as they emerge and before deployment on the production node, thereby helping you with the vulnerability management and improved security posture of your production network.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 707, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b81de390c041029e6b2add61bd9dfd2a', 'text': '• Securing 5G CNF images: You should ensure that the vendor you choose as a part of the 5G deployment has a process in place that ensures all the container images are scanned for any vulnerabilities. They should also have a procedure to track all the Common Vulnerabilities and Exposures (CVEs) in the shipped images and provide resolution if any CVEs are detected. For efficient vulnerability management of 5G CNFs, it is recommended to use risk-based vulnerability management (RBVM) solutions available in the market today, which provides a risk score factoring in the number of instances of each vulnerability in your environment, their potential severity, and the assets that are threatened as a result of each vulnerability. Having such solutions in place will help you better manage the risks in 5G CNF deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 707, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '98f53fb5137f95962e723805e376e62c', 'text': '• Secure registry management: The vendor should ensure that the images are scanned, approved, and signed before being uploaded to the image registry. This should be followed for both 3GPP and non-3GPP NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 707, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd09004abf46e52a1235a849cd5a1a01f', 'text': "• Secure software delivery: The vendor should ensure that they enforce authentication mechanisms to limit distribution to specific customers only based on the SLA and other agreements. As an example, the software from the vendor's software download site should have a stringent authentication mechanism to ensure that only legitimate customers are downloading the software.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 707, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0fc2aa0f849a2ae9c743cf12e901c93b', 'text': '• Container and resource isolation: Isolation for CNF deployments can be implemented at different levels. Some isolations are dependent on the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 707, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bf1785df04c7d22c061758272f6b25b2', 'text': 'vendor, and some require best practices of CNF deployments. An example of isolation provided by the vendor is the container isolation provided to you by using the Kubernetes platform, which enables you to set CPU- relative priority within the CFS scheduler, maximum memory limits, and limits on persistent storage. The main aim of providing granular isolation such as container isolation is to protect your host OS and mitigate against malicious container escape and breakout attempts into other targets hosted on the same host. As an example, the vendor should provide you with options for controlling pod placement. Pods are the rough equivalent of a machine instance (physical or virtual) to a container. Each pod is allocated its own internal IP address, thus owning its entire port space, and containers within pods can share their local storage and networking. In methods such as OpenShift, you are provided with an option for controlling pod placement. In OpenShift, the Pod Node Constraints Admission Controller ensures that pods are deployed onto only specified node hosts using labels, and it prevents users without a specific role from using the nodeSelector field to schedule pods. Using this feature, a cluster administrator can set a policy to prevent application developers with certain roles from targeting specific nodes when scheduling pods. This level of isolation will ensure that rogue application developers working on non-3GPP 5G NFs cannot interfere with your pods with 5G 3GPP NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 708, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd517829b7ff24e20a4762808645eaa23', 'text': '• User-to-application mapping: The vendor you choose as a part of your 5G deployment should allow granular user access to mitigate the risk of unauthorized access to applications in your network. In a container environment, Kubernetes does not implement any kind of user privilege isolation but instead uses RBAC to enable you to configure fine-grained and specific sets of permissions that define how a given user, or group of users, can interact with any Kubernetes object in your cluster, or in a specific namespace of your cluster. Apart from RBAC, it is recommended that you also follow the user access security controls discussed earlier in the section “Securing User and Device Access Using Zero-Trust Principles.” This is critical, because once your network evolves to include hybrid deployment models, where you will implement non-3GPP and 3GPP NFs in the public cloud and private cloud, the risks of unauthorized access increases drastically and you will need a robust end-to-end granular access controls for users and devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 708, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c0274f51426dc591902607b4ec9207b0', 'text': '• Microsegmentation: Apart from the container isolation provided by the vendor, you should implement an end-to-end microsegmentation layer for', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 708, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a3a384e94ff0946ae81904f4cf7188fb', 'text': 'all the 3GPP and non-3GPP 5G NFs deployed in your network. Microsegmentation is a security best practice that offers a number of advantages over more established approaches like network segmentation and application segmentation. Microsegmentation uses much more information in segmentation policies, such as application-layer information. It enables policies that are more granular and flexible to meet the highly specific needs of an organization or business application. You can also manage and enforce rules on end-to-end connections for just a group of components in a given network segment. The added granularity that microsegmentation offers is essential at a time when many organizations are adopting new container-based environments that make traditional perimeter-based security less relevant. By segmenting the network communication between pods, you can control the flow of traffic, allowing or blocking traffic based on a variety of factors. Segmented networks can reduce the attack surface by containing certain traffic only to portions of the network, and they can prevent unauthorized network traffic or attacks from reaching portions of the network to which they would prefer to prevent access. Microsegmentation also makes the job of monitoring network traffic much easier. Using microsegmentation to implement a zero-trust architecture will involve a paradigm shift and some technical challenges, but it will improve the following aspects of your network security:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 709, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d4856cacbbf6adaa5dfb8ffbc0660b4', 'text': '• As containers are often deployed as microservices and can be dynamically deployed and scaled across a Kubernetes cluster, segmenting containers should be done on the service level. Because different services can be deployed across shared networks and servers (or VMs and hosts), and each workload or pod has its own network addressable IP address, container segmentation policies can be difficult to create and enforce with the existing network-based solutions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 709, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7c1b8c29ef62cb849d533d7ff7af0c52', 'text': '• You can gain control and visibility over which workloads the open source tools consist of and who they are communicating with.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 709, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '90dff13590688185fa7f729d87e650ef', 'text': "• Namespaces have been found to be useful for organizing services and to ease the management of services, where each one in a namespace has some attributes in common with others. Creating separate namespaces is an important part of isolation; however, it adds little security and doesn't restrict workload activity. This requires", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 709, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '53e5cc3ec6e9b06dd78aefc343766675', 'text': 'additional microsegmentation strategies to be implemented to apply granular microsegmentation policy to workloads.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 710, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '260fa167e1119233b8a3fbf407953e76', 'text': '• Service Mesh: To have a solid cloud-native application security strategy, you should make use of innovations in the cloud-native industry, which provides more granular security controls over applications. One of the key innovations is the service mesh. The use of cloud-native function in 5G deployments creates new security challenges. With microservices being updated much more frequently than they have in the past, service providers who struggled with microsegmentation when dealing with a few VMs for 4G deployments will face greater challenge with 5G NFs, which run dozens of containers that are being updated more frequently. Adoption of service mesh will provide you with a reliable and consistent way to connect, observe, and apply granular microsegmentation to your microservices. It provides you with other key features such as service-to- service authentication, policy creation, load balancing, and traffic routing. It will help to abstract the network topology and routing away from the infrastructure layer and build it into the network function/application itself by adding a sidecar proxy to the application, which abstracts the inter- service communications as well as monitoring and security to the workload. If you are a developer building applications to fulfill 5G customer use cases, a service mesh will allow you to easily link together microservices using a declarative model-based approach that sits on top SDN layers and traditional layers in the underlying infrastructure. At press time, the most popular service mesh is Istio, the open source code started by Google, Lyft, and IBM. There are other service mesh options, such as Consul, Linkerd, Kuma, AWS Mesh, and Open Service Mesh.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 710, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d5700bf89eccde07b03de50126c56a0', 'text': 'Table 10-5 provides a checklist for securing both 3GPP and 3GPP applications —VNFs, CNFs, and third-party applications.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 710, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '0a01165b7288d952e036296aa91e9947', 'text': 'Recommended Security Does This Security Solution/Feature Used Controls Control/Capability Exist in Your Network? (Y/N) Hardened software and hardware Visibility on VNF and CNF interactions (control plane) Visibility on API calls and encrypted traffic Secure 5G CNF images Secure registry management Visibility on multistack public and private cloud interactions (control plane) Malware detection on encrypted data (control plane) Microsegmentation', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Recommended Security Controls</th><th>Does This Security Control/Capability Exist in Your Network? (Y/N)</th><th>Solution/Feature Used</th></tr></thead><tbody><tr><td colspan="3">Hardened software and hardware</td></tr><tr><td colspan="3">Visibility on VNF and CNF interactions (control plane)</td></tr><tr><td colspan="3">Visibility on API calls and encrypted traffic</td></tr><tr><td colspan="3">Secure 5G CNF images</td></tr><tr><td colspan="3">Secure registry management</td></tr><tr><td colspan="3">Visibility on multistack public and private cloud interactions (control plane)</td></tr><tr><td colspan="3">Malware detection on encrypted data (control plane)</td></tr><tr><td>Microsegmentation</td><td></td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 711, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '2cb8c3866bb661a9141be3a61f4c8707', 'text': "RBAC TLS 1.3 encryption Authentication between SGC CNFs (both 3GPP and non- 3GPP) API gateway Web application firewall for API Security policy enforcement per VNF/container User-to-application mapping (including containers) Secondary authentication (for slice-specific authentication) Slice-level isolation of CNFs|md]physical separation of CNF's (design methodology) Multifactor user authentication", 'metadata': {'text\_as\_html': "<table><thead><tr><th>RBAC</th></tr></thead><tbody><tr><td>TLS 1.3 encryption</td></tr><tr><td>Authentication between SGC CNFs (both 3GPP and non- 3GPP)</td></tr><tr><td>API gateway</td></tr><tr><td>Web application firewall for API</td></tr><tr><td>Security policy enforcement per VNF/container</td></tr><tr><td>User-to-application mapping (including containers)</td></tr><tr><td>Secondary authentication (for slice-specific authentication)</td></tr><tr><td>Slice-level isolation of CNFs|md]physical separation of CNF's (design methodology)</td></tr><tr><td>Multifactor user authentication</td></tr></tbody></table>", 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 712, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '182be643f323abe523c3b78238e3e9e6', 'text': 'Runtime Application Self- Protection (RASP) as part of DevSecOps process Static application software testing (SAST) as part of DevSecOps process Dynamic application software testing (DAST) as part of DevSecOps process Automated continuous integration/continuous delivery (CI/CD) CNF image scanning Vulnerability management (including application development stage) Compliance management (including 5G VMs and container deployments) Forensics (including 5G VMs and container deployments)', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Runtime Application Self- Protection (RASP) as part of DevSecOps process</th></tr></thead><tbody><tr><td>Static application software testing (SAST) as part of DevSecOps process</td></tr><tr><td>Dynamic application software testing (DAST) as part of DevSecOps process</td></tr><tr><td>Automated continuous integration/continuous delivery (CI/CD)</td></tr><tr><td>CNF image scanning</td></tr><tr><td>Vulnerability management (including application development stage)</td></tr><tr><td>Compliance management (including 5G VMs and container deployments)</td></tr><tr><td>Forensics (including 5G VMs and container deployments)</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 713, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1b181f0df1ebb614cc6e3a5faa855a2d', 'text': 'Table 10-5 Security Control Checklist for Application Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 713, 'parent\_id': 'abeea7a6ac96cd2cef5bcb78586865da', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '36749984378e1475536d5a3729180637', 'text': 'Vulnerability Management and Forensics', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 713, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '38ea873250ca794782404750a1d64611', 'text': '5G NF deployment based on Cloud-Native Functions (CNFs) brings in risk vectors due to open source software being used to build 5G NFs and applications. Because the 5G NFs and applications can run anywhere from on-', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 713, 'parent\_id': '36749984378e1475536d5a3729180637', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cb168ddfdf2b7858ce9555964a2625ea', 'text': 'premises to multicloud and cloud-native microservices, combined with accelerated innovation, the need for an application-led approach to security is paramount. You will need to identify vulnerabilities within the application during production, correlate vulnerabilities and breaches with business impact, and bring together the application and security teams to facilitate speedy remediation. Implementing an application-aware vulnerability detection and forensics layer that can identify vulnerabilities across the physical and virtual infrastructure (including virtual machines and container deployments) is critical. You should follow a DevSecOps model to develop security automation that scales directly alongside your deployment methods, be it an on-premises, cloud, or hybrid model, so that you can ensure security standardization and architectural strength at scale.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 714, 'parent\_id': '36749984378e1475536d5a3729180637', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b0a3167aca49a1f61ae07b0e7896aaaa', 'text': 'Figure 10-9 illustrates an example of implementing vulnerability detection and forensics in 5G deployment which has both software-defined network (SDN) and non-SDN components. The data and log collection system will collect the non-SDN network and application telemetry in the form of IP network traffic telemetry (for example, NetFlow, S-flow and so on), hypervisor metadata, container sidecar telemetry, and virtual private cloud (VPC) logs. The data and log collection system will also filter the data and apply methods like packet de- duplication. The packet broker (PB) will collect all the network telemetry (similar to the data and log collection system) and optimize the flow collection from the SDN layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 714, 'parent\_id': '36749984378e1475536d5a3729180637', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2556130bcac482052dc9a3e644918539', 'text': 'The collected telemetry from the data and log collection system and packet broker is then fed into the vulnerability detection and forensics solution, which has integrations with threat intelligence (which provides you with a list of threats and threat actors), the Common Vulnerabilities and Exposure (CVE) database (a list of publicly disclosed computer security flaws), your custom policy defined for the network, and machine learning (ML) and artificial intelligence (AI) to detect all the vulnerabilities and list them based on the risk factor. All these integrations with the vulnerability management and forensics solution will help you to detect any vulnerabilities with much higher accuracy and apply forensics investigations when required.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 714, 'parent\_id': '36749984378e1475536d5a3729180637', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f8d1a1dcb9da6a462516710325951c9e', 'text': 'Policy defined Thieat CVE for Applcation Al Intel 0B 1ERR Alert Corrt Actio Packet Broker (PB) | e PB controller Nebwork Telemety \_,, O — (Edge + Central DC) é E A A Optical TAP / SPAN REST AP! | SON Controller Network Telemetry Container Telemelry Hypenvisor metadata EEO T R0 — Cloud Telemetry 00,0y 66, 70 | | VRAN Apps | upe | MECA i | Packet Core Apps pps = E E | : ........... =W \\ o 7 | Ll ((A)) w@ Wbas @ bt @ oy L] ] Jell Sites Far Edge DC Edge 0C Central DC Off-Prem', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 715, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bc58b4f188a3e39ad58865099293ed0c', 'text': 'Alert Corrt Actio', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 715, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '41e5264083ce7275f95ad42d423de7b6', 'text': 'Alert', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 715, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'd7852eed144d057e73ce94780ed4364c', 'text': 'Figure 10-9 Vulnerability Management and Forensics', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 715, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9879efeb4958658f314d41870dc08109', 'text': 'The solution you choose for vulnerability management and forensics should allow you to perform the following key functions:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 715, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '686c19ef1d6d723fcf48df36644b31eb', 'text': '• Perform continuous monitoring of the end-to-end network components (hardware and software) to detect any anomalous events, behaviors, and malware', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 715, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '938551f0749baac7427f1384639cd384', 'text': '• Baseline the behavior or the workloads based on communication activities and processes on the workloads', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 715, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b4e280581cc6066e499b7baf30e293ed', 'text': '• Proactively detect anomalous behavior and identify indicators of compromise', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 716, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e8a658ee19404895c411003e4c449b90', 'text': '• Allow custom definition of critical components', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 716, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd7ba7685b13c091f8d1f897990d224b2', 'text': '• Prioritize vulnerability and patch management based on criticality of the network component', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 716, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2ab1252bce670cfff42712f259b9bacd', 'text': '• View aggregated information about network security risks and vulnerabilities relevant to a specific business application', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 716, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '20d576d8154e25bfddef287a6917e6f5', 'text': '• Get a baseline of the software inventory and the version information', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 716, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '09921b848d5a2635643feaca64d6c3c5', 'text': '• Identify any of the package versions that have known vulnerabilities or exposures, along with their severity', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 716, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '82a3e566e3f5d2e3c0040ab1678015d7', 'text': '• Get an accurate inventory of all the servers that have the vulnerable package and map it to a policy that designates a specific action, such as updating firewall rules or other infrastructure elements to enforce relevant policy elements', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 716, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '44cd7fb702044bd5e6ea381b2d054884', 'text': '• Enable vulnerability alerts to be integrated with your security information and event management (SIEM) systems for further security incident handling', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 716, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8e91ff34503e4b149fa14b63590ce0aa', 'text': '• Allow integration with patch management solutions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 716, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ceec9508d2fd3bdc13a0030da7f304f2', 'text': 'Table 10-6 is a checklist for providing vulnerability management and forensics for your end-to-end 5G deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 716, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'eabb9e508654aed53741a8dec7cbfcd9', 'text': 'Recommended Security Controls Does This Security Solution/Feature Control/Capability Used exist in Your Network? (Y/N) Vulnerability management of CNFs deployed in multicloud stack Vulnerability management of VNFs and CNFs deployed on VMs Vulnerability management of VNFs and CNFs deployed on bare metal (BM) Forensics capability on VNFs and CNFs Automated capability of consolidating, de-duplicating, and correlating vulnerabilities Automatically identify and fix vulnerabilities in containers Full lifecycle vulnerability scanning (including the build, ship, and CI/CD pipeline and runtime)', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Recommended Security Controls</th><th>Does This Security Control/Capability exist in Your Network? (Y/N)</th><th>= Solution/Feature Used</th></tr></thead><tbody><tr><td colspan="3">Vulnerability management of CNFs deployed in multicloud stack</td></tr><tr><td colspan="3">Vulnerability management of VNFs and CNFs deployed on VMs</td></tr><tr><td colspan="3">Vulnerability management of VNFs and CNFs deployed on bare metal (BM)</td></tr><tr><td colspan="3">Forensics capability on VNFs and CNFs</td></tr><tr><td colspan="3">Automated capability of consolidating, de-duplicating, and correlating vulnerabilities</td></tr><tr><td colspan="3">Automatically identify and fix vulnerabilities in containers</td></tr><tr><td>Full lifecycle vulnerability scanning (including the build, ship, and CI/CD pipeline and runtime)</td><td></td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 717, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8065e023df6e41834c10d609e8ea89f4', 'text': 'Table 10-6 Security Control Checklist for Vulnerability Management and Forensics', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 717, 'parent\_id': 'd7852eed144d057e73ce94780ed4364c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b06bead0f89704af561a17777c7d975e', 'text': 'Enhanced Visibility, Monitoring, and Anomaly Detection', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 717, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7f1efd5ccfddec651c74b598225924e2', 'text': 'One of the primary security controls is end-to-end visibility. Without the visibility of the end-to-end components, it is very hard to detect any threats or any unusual behavior in the infrastructure. If you do not have the visibility of the entire network, it will create blind spots that can cause infiltration of the', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 717, 'parent\_id': 'b06bead0f89704af561a17777c7d975e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '22624c2b17cebfeabde89bbcd7bb21fa', 'text': 'malicious traffic into your infrastructure and cause serious damage to the network or data exfiltration of sensitive data. Figure 10-10 illustrates the key interfaces that require visibility in your 5G deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 718, 'parent\_id': 'b06bead0f89704af561a17777c7d975e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a78e17ecb46130298063d5828c89dc79', 'text': 'amm—— 5G Mobile Network essssessssessssesasaannnna. B28,82C, B2H, B2B2X 5GC (Public Cloud/ On- =4 premises MEC (Public Cloud/ On- Management, Orchestration, premises) SON ’\_Q\_N Data Network [ Internet SLssssssssssssssssssssssssssssssssssssssssssssssssasse”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 718, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0c4559ea0efb184acdd52bbb64499f0e', 'text': 'Figure 10-10 End-to-End Visibility of 5G Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 718, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5787b9053d98f2e7d30d7d632e3c4079', 'text': 'By ensuring visibility in the interfaces shown in Figure 10-10, you can continuously monitor and detect advanced threats that have either bypassed existing security controls or originate from within. Monitoring of these network devices and interfaces can be carried out by capturing network telemetry and analyzing the network packet metadata. Network packet', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 718, 'parent\_id': '0c4559ea0efb184acdd52bbb64499f0e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8e8da6975dfe5e2acb3c1d5eb2c1ab1c', 'text': 'metadata can provide useful insights about who is connecting to the organization and what they are up to. Everything touches the network, so these insights can extend from the HQ to the branch, public cloud, and private data centers, roaming users, and even IoT. Analyzing this data can help detect threats that might have found a way to bypass your existing controls, before they are able to have a major impact. Analyzing this data will also help you detect questionable behavior undertaken by hostile insiders. Properly functioning analytics can lessen the burden on your security team and provide them with more opportunity to concentrate on high-probability threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 719, 'parent\_id': '0c4559ea0efb184acdd52bbb64499f0e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e7c7b9fb3bf2405b6a6e9b5535fb358', 'text': 'Figure 10-11 illustrates an example of continuous monitoring for the 4G and 5G packet core. The data and log collection includes flows from various devices, network equipment (both SDN and non-SDN related), and CNF applications used for 5G deployment. Apart from the telemetry from CNFs and network equipment, it is also important to get the system logs (syslog) and network security event logs (NSEL) from the firewalls, web application firewalls, and encrypted traffic analytics (ETA) to identify malware within encrypted traffic without having to decrypt the data traffic. All this collected data is then sent to the enhanced visibility and anomaly detection layer solution. The enhanced visibility and anomaly detection layer solution first creates the baseline of the network by understanding the management, service, and control plane behavior for 2 or 3 weeks, sometimes up to a month if your network is complex and includes multiple layers technologies, such as Wi-Fi, 2G, 3G, 4G, 5G NSA, and 5G SA deployments. Once the baseline is measured and identified, along with the policy defined by you, any variations of traffic against the baseline can be deemed an anomaly. This anomalous traffic is then inspected using ML and AI algorithms to ascertain the legitimacy of and to identify any malware. If any malware is identified, the impacted hosts can then be moved into a quarantine layer to prevent any lateral movement.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 719, 'parent\_id': '0c4559ea0efb184acdd52bbb64499f0e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '264eab51b14d49b12ced6c1392c4b6e4', 'text': 'The orchestration layer uses a policy-driven approach to automate the network resource allocation to deliver a service or application. Orchestration allows networks to scale as needed, enables network services to be provisioned across multiple devices, and makes it possible to deploy resources as needed, thus making the network more agile and responsive. An API is the most common interface for interactions between the EPC and 5GC to the orchestration layer. A web application firewall or API gateway will provide you with enhanced API visibility and are two major inline security tools for API protection.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 719, 'parent\_id': '0c4559ea0efb184acdd52bbb64499f0e', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5b60ee6a6a0ba69ce5f616df738cf96f', 'text': '1ER —— Enhanced Visibiity & Anomaly Detection Engine L] cem D. Data & Log Collection L L] T L Myl L TS Device flows ! é NSEL, Syslog, device flow, metadata ........................................................................ | é APIGW/WAF APIGW | WAR asdsccssannsensnantaannnanans NSEL, Syslog NGFW NGFW Centralized 4G & 5GC Application-Level [ ETA flows Polcy Enforcement ngine Workload and flow feeds, Policy enforcements Device flows (Netflow, C-flow efc..), VM metadata, | é Sssssasssssssassssssssssssssasssssassssssasasssssasssssssassssshanassasaanassannansadnal Container Flow telemety, Service Mesh Telemetry', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 720, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '76b5cda11dd33619719945437402cb39', 'text': 'Figure 10-11 End-to-End Monitoring of 4G and 5G Packet Core', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 720, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9a1218bab523050ace7163699f05a7fd', 'text': 'Figure 10-12 illustrates an example of end-to-end continuous monitoring for ORAN/VRAN deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 720, 'parent\_id': '76b5cda11dd33619719945437402cb39', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '628311bc34c2dc4b3a03fe692b4af70b', 'text': 'Palicy defined Threat for Application Al Intel EER Alert Enhanced Visibilty & = Com Anomaly Detection Engine Actio | PR— PB controller O — = Nebwork Telemety \_,, Data & Log Collection (Edge + Central DC) | S — i E 0 A A ! | Optical TAP / SPAN RESTAPI | Network Telemetry SON Controller Container Telemelry Hypenvisor metadata =3 ERe 3R 23 =3 2R pre— R— Cloud Telemetry Du,Cu | 8¢, EPC VRAN Apps | o, e D | | Packet Core Apps | MEC Apps % e E é i \\ L. ﬁ / Neoesossees g ; a e [ [ | . ((A)) F Midhaul WAN ([ ] @ ( Backhaul 8 Sell Sites FarEdge DC Edge DC Central DC Off-Prem', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 721, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '01193e52b42488171c237183c8c6c6e4', 'text': 'Figure 10-12 End-to-End Visibility of 5G ORAN Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 721, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5f64fab35d9ab362c00bd8fd20ef0b87', 'text': 'As shown in Figure 10-11, the monitoring layer should include both software- defined network (SDN), non-SDN, and legacy network devices. Having a packet broker in your monitoring architecture would highly optimize the flow collection. For example, suppose you need to monitor only the control, service, and management plane; in this case you can drop all the other traffic (for example, user plane) using the customizable filtering rules in the packet broker and then monitor only the control plane traffic. This will optimize the number of flows required to be sent to your SIEM layer, thereby reducing your cost, as the SIEM vendors generally has pricing models based on volume of data ingested by the SIEM solution.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 721, 'parent\_id': '01193e52b42488171c237183c8c6c6e4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0d138bc0c2c8af8bf642e11692452751', 'text': 'Alert', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 721, 'parent\_id': '01193e52b42488171c237183c8c6c6e4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '573037d4624cddad7525119af635d476', 'text': 'Com Actio', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 721, 'parent\_id': '01193e52b42488171c237183c8c6c6e4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e39e7b028696750a3a715deef9853b66', 'text': 'It will also help you to respond quickly and effectively with complete knowledge of threat activity, network audit trails for forensic investigations, and integration with existing security controls. End-to-end monitoring can help you with your Governance, Risk and Compliance (GRC) requirements, specifically it will help you to detect any regulatory and internal policy violations. You should create policy violation alarms tuned to your required business logic to ensure you capture the relevant anomalies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 722, 'parent\_id': '01193e52b42488171c237183c8c6c6e4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2e8f02f7df5d96659d512ee715d8c885', 'text': 'Table 10-7 provides a checklist for ensuring granular monitoring and anomaly detection for your end-to-end 5G deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 722, 'parent\_id': '01193e52b42488171c237183c8c6c6e4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '3aca58e4968432fce19f88093d1615fe', 'text': 'Recommended Security Controls Does This Security Solution/Feature Control/Capability Used Exist in Your Network? (Y/N) Visibility in control plane for inter- VNF, CNF communications NFVi visibility Anomaly detection Detecting anomalies in encrypted traffic without decryption (including encrypted APl communication) Encrypted traffic malware detection (without need for decryption) Detection of rogue/fake eNB, gNB, and MEC gateway Monitoring of cloud-deployed 5G CNFs Visibility in control plane for inter- VNF, CNF communications Storage of collected network telemetry, syslogs, and network security event logs from firewalls', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Recommended Security Controls</th><th>Does This Security Control/Capability Exist in Your Network? (Y/N)</th><th>= Solution/Feature = Used</th></tr></thead><tbody><tr><td colspan="3">Visibility in control plane for inter- VNF, CNF communications</td></tr><tr><td colspan="3">NFVi visibility</td></tr><tr><td colspan="3">Anomaly detection</td></tr><tr><td colspan="3">Detecting anomalies in encrypted traffic without decryption (including encrypted APl communication)</td></tr><tr><td colspan="3">Encrypted traffic malware detection (without need for decryption)</td></tr><tr><td colspan="3">Detection of rogue/fake eNB, gNB, and MEC gateway</td></tr><tr><td colspan="3">Monitoring of cloud-deployed 5G CNFs</td></tr><tr><td colspan="3">Visibility in control plane for inter- VNF, CNF communications</td></tr><tr><td>Storage of collected network telemetry, syslogs, and network security event logs from firewalls</td><td></td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 723, 'parent\_id': '01193e52b42488171c237183c8c6c6e4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '25e96549268411c6383b6d30b95c570f', 'text': 'Table 10-7 Security Control Checklist for Enhanced Visibility, Monitoring, and Anomaly Detection', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 723, 'parent\_id': '01193e52b42488171c237183c8c6c6e4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '76095759902eeffa644eaba22ad244e7', 'text': 'Slice-Level Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 723, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6aa50a6ed14ff336948d74d3c4c37bab', 'text': 'The openness and flexibility of 5G architecture allows you to peel off certain parts of your network to provide dedicated services to industry verticals and mobile service consumers. It also allows you to integrate with an enterprise or', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 723, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '051dccb925d2a8f4840f23341020cfbd', 'text': 'industry vertical that owns and has deployed certain components of the 5G infrastructure. This kind of integration and level of abstraction also allows you to have multiple business models to monetize your 5G deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 724, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f7908c25bc3b70905921e85eb2f1bbbb', 'text': 'Models like NSaaS enables network slice consumers (communication service consumers) to manage the parameters for their networks. Another option is for network slice providers (communication service providers) to manage the parameters for the CSC network, depending on the SLA between the CSP and CSC.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 724, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '08a955582d0844e3b52ca50ddd9bc26a', 'text': 'Deployment of slicing and the business models introduces a completely different risk vector that you never had to think about in a traditional network deployment. Some of the key risks are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 724, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ebf8c5ab977fc9f21e69a3d7adf8dd2a', 'text': '• Improper management isolation in a multitenant environment, specifically for the management of the service layer in NSaaS use cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 724, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '568e2e4e9218484314cfc5d379906ffb', 'text': '• Improper slice-level isolation (both intra- and inter-slices)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 724, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'eee059e0ab1905ed6dbcd6df31dc7fe2', 'text': '• Improper slice-level authentication and authorization controls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 724, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7b0e8c54d48022e8664854b4da9d5290', 'text': '• Improper implementation of APIs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 724, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '384228710e83bb4ec934ab66e2fec431', 'text': '• DDoS attacks at the data plane and control plane', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 724, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd64824807b632396998bce6fd129dad3', 'text': 'To mitigate the aforementioned key risks, the following key security controls and deployment best practices should be implemented:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 724, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '181435a03654f22f16cfb39305d2dc10', 'text': '• Securing network slices requires you to take a holistic view toward security. You will first need to understand the use case the CSC is aiming to fulfill by using network slice components and then deciding on the security controls and capabilities for the architecture. A similar architecture consisting of RAN, back haul, MEC, and 5G packet core being deployed for different use cases will need different security controls based on the deployment model for the use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 724, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd7b28cc3596dc11fe1adac71340731ae', 'text': 'For example, consider a CSP providing parts of 5G network functions such as User Plane Functions (UPFs) and Control Plane Functions like AMF and SMF, while your customer (such as the industry vertical CSC) has deployed its own 5G radio access nodes (gNB) to cater for sensors in a critical infrastructure deployment. In another use case, you are providing your subscribers an eMBB slice to cater for their requirements of broadband usage. Here, although the same network components used are similar, apart from the gNB already deployed by CSC, the security controls are quite', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 724, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5012dfe0c9f796329cc3689fdd3ae838', 'text': "different. In the case of the industry vertical CSC, apart from the security considerations that you have planned for the subscriber's user equipment DDoS attacks, you will also need to cater for granular access control of industry vertical CSC users accessing the management in the service layer of the NSaaS.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 725, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '59fdf876f4e30525425547b622d6ef40', 'text': '• Ensuring granular access control on the management within the service layer for NSaaS is very important because any unauthorized access on the management within service layer or insufficient access control could lead to illegitimate users from one CSC having access to slice management of another CSC, thus leading to leakage of sensitive data or slice sabotage, where the NFs of the slices could be deleted or destroyed, leading to loss of service.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 725, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ec2589c6a3c2bcef7c079e04e9a0232e', 'text': '• Another aspect to consider for secure network slicing is the security of the orchestration and SDN components assisting in the deployment and operation of the network slices. The orchestration and SDN layers use API calls in the majority of communications. These APIs are prone to weak security implementation by the developers and vulnerabilities in the API web servers. Best practices for deploying APIs, such as using HTTP over TLS, should be considered to provide secure connectivity. Granular access control should be implemented for the orchestration and SDN layers, as any unauthorized access to these layers could cause serious disruption to the network. An entire slice could be destroyed or deleted by the malicious unauthorized user causing a denial of service.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 725, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1039b703dfc6325e96531efdb117285f', 'text': '• The SDN data plane is a part of the network slice that is prone to DDoS attacks from devices within the network infrastructure and outside the network. This can be mitigated by providing a DDoS detection and protection mechanism at the Internet-facing interfaces and implementing rate limiting at the application level. The SDN layer should also include Control Plane Policing methods to mitigate any attack at the control plane layer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 725, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1dcb67b0fed862792660562b033bc179', 'text': '• Depending on the use case and the location of deployment of 5G slice NFs, side-channel attacks could be a major concern. This is of particular importance for URLLC use cases, where MEC applications are deployed closer to the user. In industry vertical use cases such as smart manufacturing, these MEC applications could be deployed in an on- premises DC. To mitigate data exfiltration using side-channel attacks,', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 725, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e5df37acade12a071da5e1253786b086', 'text': 'enhanced visibility layer, including anomaly detection in encrypted traffic, should be implemented.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 726, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '92b9cc5e7f26812655b7ae5538dea1b4', 'text': 'Table 10-8 provides a checklist for securing network slice deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 726, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '1448296f81e222598d93f4197b30d1b3', 'text': 'Recommended Security Controls Does This Security Solution/Feature Used Control/Capability Exist in Your Network? (Y/N) Slice-level secondary authentication Slice-level isolation of CNF Slice-level visibility Secure APl in orchestration and SDN layers DDoS protection for NSaaS offerings Slice- level Granular Access Control for devices and applications', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Recommended Security Controls</th><th>Does This Security Control/Capability Exist in Your Network? (Y/N)</th><th>= Solution/Feature Used</th></tr></thead><tbody><tr><td colspan="3">Slice-level secondary authentication</td></tr><tr><td colspan="3">Slice-level isolation of CNF</td></tr><tr><td colspan="3">Slice-level visibility</td></tr><tr><td colspan="3">Secure API in orchestration and SDN layers</td></tr><tr><td colspan="3">DDoS protection for NSaaS offerings</td></tr><tr><td>Slice- level Granular Access Control for devices and applications</td><td></td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 726, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ebadd3665665110de5f4affbc3fc68ef', 'text': 'Table 10-8 Security Control Checklist for Slice Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 726, 'parent\_id': '76095759902eeffa644eaba22ad244e7', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '394d07261dca10c3e913de92a3f1ec5d', 'text': 'Secure Interoperability', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 726, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5483b92154e62b6390603599c0302d6e', 'text': 'Although this book is aimed at 5G, you should also consider pragmatic deployment models that include integrations with 4G. As an example, the roaming deployment in 5G considers Security Edge Protection Proxy (SEPP), which ensures end-to-end confidentiality and/or integrity between the source and destination network for all 5G interconnect roaming messages. In real deployments, however, there is still some time before we can have widely deployed 5G networks and thus 5G roaming partners. The roaming scenario will be primarily dominated by 2G/3G/4G for a few more years. This means that the GTP, Diameter, and SS7 firewalls should not be discounted and should be planned at the roaming peering points to mitigate risks related to roaming attacks prevalent in legacy technologies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 726, 'parent\_id': '394d07261dca10c3e913de92a3f1ec5d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '25bf3ad05c5dcf070db6f913d20fdd57', 'text': 'Table 10-9 provides a checklist for securing interoperability with roaming partners and other public networks.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 727, 'parent\_id': '394d07261dca10c3e913de92a3f1ec5d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '84796891ef5213f05a22f1ede4d1ad98', 'text': 'Recommended Security Controls Does This Security Solution/Feature Control/Capability Used Exist in Your Network? (Y/N) GTP inspection (if you still have 4G network or roaming with 4G networks) SCTP inspection (if you still have 4G network or roaming with 4G networks) Diameter inspection (if you still have 4G network or roaming with 4G networks) SS7 inspection (if you still have 2G network or roaming with 2G networks) Security Edge Protection Proxy (SEPP) Service Communication Proxy (SCP)', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Recommended Security Controls</th><th>Does This Security Control/Capability Exist in Your Network? (Y/N)</th><th>| Solution/Feature Used</th></tr></thead><tbody><tr><td colspan="3">GTP inspection (if you still have 4G network or roaming with 4G networks)</td></tr><tr><td colspan="3">SCTP inspection (if you still have 4G network or roaming with 4G networks)</td></tr><tr><td colspan="3">Diameter inspection (if you still have 4G network or roaming with 4G networks)</td></tr><tr><td colspan="3">SS7 inspection (if you still have 2G network or roaming with 2G networks)</td></tr><tr><td colspan="3">Security Edge Protection Proxy (SEPP)</td></tr><tr><td>Service Communication Proxy (SCP)</td><td></td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 727, 'parent\_id': '394d07261dca10c3e913de92a3f1ec5d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f0556170fbc11024415615113a2946f', 'text': 'Table 10-9 Security Control Checklist for Interoperability', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 727, 'parent\_id': '394d07261dca10c3e913de92a3f1ec5d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c536cf0d88ac8dca7401ea42d619a1b0', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 727, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5e4612e3aab069460334911b6c1f876f', 'text': 'As discussed in this chapter, building a pragmatic security architecture requires you to understand the type of deployment model (on-premises, public cloud, or hybrid), the architecture being deployed (Distributed RAN, ORAN, and so on), and the use cases being implemented.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 727, 'parent\_id': 'c536cf0d88ac8dca7401ea42d619a1b0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'caba058b660f0a501e95ba0c6f8d70a0', 'text': 'Furthermore, you also need to consider the existing legacy technologies already existing in your network. Table 10-10 explains the recommended security controls for multiple radio access technology (multi-RAT) deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 727, 'parent\_id': 'c536cf0d88ac8dca7401ea42d619a1b0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'de3d6c357a8dce8667cd0c2cc968d118', 'text': 'Security Control 2G 2G + 3G 2G +3G + 2G +3G + 4G 4G + 5G Centralized security v gateway Distributed security gateway DIAMETER inspection SCTP inspection GTP inspection Carrier-grade NAT N Web application firewall (WAF) DDoS Gi-Firewall SS7 security Visibility on packet NSNS core (CP) Multifactor AN Authentication Network slice security DNS security endpoints Application security AN < N API security Vulnerability management Management/DCN security Microsegmentation Supply chain security AIARIEARNATNTATAIAND', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Security Control</th><th>2G</th><th>2G + 3G</th><th>2G +3G + 4G</th><th>2G +3G + 4G +5G</th></tr></thead><tbody><tr><td>Centralized security gateway</td><td></td><td></td><td>v</td><td></td></tr><tr><td>Distributed security gateway</td><td></td><td></td><td></td><td></td></tr><tr><td>DIAMETER inspection</td><td></td><td></td><td></td><td></td></tr><tr><td>SCTP inspection</td><td></td><td></td><td></td><td></td></tr><tr><td>GTP inspection</td><td></td><td></td><td></td><td></td></tr><tr><td>Carrier-grade NAT</td><td></td><td></td><td>N</td><td></td></tr><tr><td>Web application firewall (WAF)</td><td></td><td></td><td></td><td>MR</td></tr><tr><td>DDoS</td><td></td><td></td><td></td><td></td></tr><tr><td>Gi-Firewall</td><td></td><td></td><td>NSNS</td><td></td></tr><tr><td>SS7 security</td><td>N</td><td>N</td><td></td><td></td></tr><tr><td>Visibility on packet core (CP)</td><td></td><td></td><td></td><td></td></tr><tr><td>Multifactor Authentication</td><td></td><td></td><td>AN</td><td></td></tr><tr><td>Network slice security</td><td></td><td></td><td></td><td></td></tr><tr><td>DNS security endpoints</td><td></td><td></td><td></td><td></td></tr><tr><td>Application security</td><td></td><td></td><td></td><td></td></tr><tr><td>API security</td><td>AN</td><td>&lt;</td><td>N</td><td></td></tr><tr><td>Vulnerability management</td><td></td><td></td><td></td><td></td></tr><tr><td>Management/DCN security</td><td></td><td></td><td></td><td></td></tr><tr><td>Microsegmentation</td><td></td><td></td><td></td><td></td></tr><tr><td>Supply chain security</td><td></td><td></td><td></td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 728, 'parent\_id': 'c536cf0d88ac8dca7401ea42d619a1b0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f64fe49d26bf560b68e08c84bbfe569e', 'text': 'Table 10-10 Security Control Checklist for Securing Multi-RAT Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 729, 'parent\_id': 'c536cf0d88ac8dca7401ea42d619a1b0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f2c3ea4966d9b000241b1c038411bdf6', 'text': 'Acronyms Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 729, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '26fca4333262a765ba0e3e72a5f49bb0', 'text': 'The following table expands the key acronyms used in this chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 729, 'parent\_id': 'f2c3ea4966d9b000241b1c038411bdf6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '4fafb8a840509ff91b0982aa6f63df61', 'text': 'Acronym Expansion 3GPP Third-Generation Partnership Project 5GC 5G Core AAU Active Antenna Unit API Application programming interface BH Back haul BM Bare metal Cc2C Control and command center CD Continuous development CGNAT Carrier-Grade Network Address Translation Cl Continuous integration CNF Cloud-Native Function cp Control plane CSC Communication service customer CSMF Communication Service Management Function CSp Communication service provider CU Centralized Unit DCN Data control network DDoS Distributed denial of service DN Data network DNS Domain Name System', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Acronym</th><th>Expansion</th></tr></thead><tbody><tr><td>3GPP</td><td>Third-Generation Partnership Project</td></tr><tr><td>5GC</td><td>5G Core</td></tr><tr><td>AAU</td><td>Active Antenna Unit</td></tr><tr><td>API</td><td>Application programming interface</td></tr><tr><td>BH</td><td>Back haul</td></tr><tr><td>BM</td><td>Bare metal</td></tr><tr><td>Cc2C</td><td>Control and command center</td></tr><tr><td>CD</td><td>Continuous development</td></tr><tr><td>CGNAT</td><td>Carrier-Grade Network Address Translation</td></tr><tr><td>Cl</td><td>Continuous integration</td></tr><tr><td>CNF</td><td>Cloud-Native Function</td></tr><tr><td>cp</td><td>Control plane</td></tr><tr><td>CSC</td><td>Communication service customer</td></tr><tr><td>CSMF</td><td>Communication Service Management Function</td></tr><tr><td>CSp</td><td>Communication service provider</td></tr><tr><td>CU</td><td>Centralized Unit</td></tr><tr><td>DCN</td><td>Data control network</td></tr><tr><td>DDoS</td><td>Distributed denial of service</td></tr><tr><td>DN</td><td>Data network</td></tr><tr><td>DNS</td><td>Domain Name System</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 730, 'parent\_id': 'f2c3ea4966d9b000241b1c038411bdf6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '8b1d3225342965fa56722c8c4b8591ae', 'text': 'DoS Denial of service DU Distributed Unit ¢eMBB Enhanced Mobile Broadband EPC Evolved Packet Core FH Front haul GTP GPRS Tunnelling Protocol HTTP Hypertext Transfer Protocol HW Hardware IloT Industry Internet of Things loT Internet of Things IR Incident response IT Information technology M2M Machine-to-machine MBB Mobile broadband MEC Multi-access edge compute', 'metadata': {'text\_as\_html': '<table><thead><tr><th>DoS</th><th>Denial of service</th></tr></thead><tbody><tr><td>DU</td><td>Distributed Unit</td></tr><tr><td>¢eMBB</td><td>Enhanced Mobile Broadband</td></tr><tr><td>EPC</td><td>Evolved Packet Core</td></tr><tr><td>FH</td><td>Front haul</td></tr><tr><td>GTP</td><td>GPRS Tunnelling Protocol</td></tr><tr><td>HTTP</td><td>Hypertext Transfer Protocol</td></tr><tr><td>HW</td><td>Hardware</td></tr><tr><td>IloT</td><td>Industry Internet of Things</td></tr><tr><td>loT</td><td>Internet of Things</td></tr><tr><td>IR</td><td>Incident response</td></tr><tr><td>IT</td><td>Information technology</td></tr><tr><td>M2M</td><td>Machine-to-machine</td></tr><tr><td>MBB</td><td>Mobile broadband</td></tr><tr><td>MEC</td><td>Multi-access edge compute</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 731, 'parent\_id': 'f2c3ea4966d9b000241b1c038411bdf6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '0a7eb83a7974a81acb5e3310df770b0d', 'text': 'MH Mid haul MitM Man in the middle MNO Mobile network operator NAT Network Address Translation NF Network Function NFVi Network Functions Virtualization Infrastructure NOP Network operator NPN Non-public network NSaaS Network slice as a service NSC Network slice customer NSMF Network Slice Management Function NSP Network slice provider NSSMF Network Slice Subnet Management Function NW Network ORAN Open Radio Access Network oT Operational technology PKI Public key infrastructure PNI- Public Network Integrated Non-Public Network NPN', 'metadata': {'text\_as\_html': '<table><thead><tr><th>MH</th><th>Mid haul</th></tr></thead><tbody><tr><td>MitM</td><td>Man in the middle</td></tr><tr><td>MNO</td><td>Mobile network operator</td></tr><tr><td>NAT</td><td>Network Address Translation</td></tr><tr><td>NF</td><td>Network Function</td></tr><tr><td>NFVi</td><td>Network Functions Virtualization Infrastructure</td></tr><tr><td>NOP</td><td>Network operator</td></tr><tr><td>NPN</td><td>Non-public network</td></tr><tr><td>NSaaS</td><td>Network slice as a service</td></tr><tr><td>NSC</td><td>Network slice customer</td></tr><tr><td>NSMF</td><td>Network Slice Management Function</td></tr><tr><td>NSP</td><td>Network slice provider</td></tr><tr><td>NSSMF</td><td>Network Slice Subnet Management Function</td></tr><tr><td>NW</td><td>Network</td></tr><tr><td>ORAN</td><td>Open Radio Access Network</td></tr><tr><td>oT</td><td>Operational technology</td></tr><tr><td>PKI1</td><td>Public key infrastructure</td></tr><tr><td>PNI- NPN</td><td>Public Network Integrated Non-Public Network</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 732, 'parent\_id': 'f2c3ea4966d9b000241b1c038411bdf6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '78a009d10058b8f22ed44cca5f0066bf', 'text': 'RASP Runtime Application Self-Protection RAT Radio access technology RBAC Role-based access control RRU Radio Resource Unit SAST Static application security testing SCTP Stream Control Transmission Protocol SDN Software-defined network SecGW Security gateway SLA Service level agreement SLS Service level specification SOC Security operations center SSL Secure Sockets Layer TLS Transport Layer Security TN Transport network UDM Unified data management UE User equipment uUpP User plane UPF User Plane Function URLLC Ultra-reliable low-latency communication V2I Vehicle-to-infrastructure V2N Vehicle-to-network v2p Vehicle-to-pedestrian vas Vehicle-to-sensor V2V Vehicle-to-vehicle V2X Vehicle-to-everything VM Virtual machine VNF Virtual Network Function VRAN Virtual Radio Access Network WAF Web application firewall', 'metadata': {'text\_as\_html': '<table><thead><tr><th>RASP</th><th>Runtime Application Self-Protection</th></tr></thead><tbody><tr><td>RAT</td><td>Radio access technology</td></tr><tr><td>RBAC</td><td>Role-based access control</td></tr><tr><td>RRU</td><td>Radio Resource Unit</td></tr><tr><td>SAST</td><td>Static application security testing</td></tr><tr><td>SCTP</td><td>Stream Control Transmission Protocol</td></tr><tr><td>SDN</td><td>Software-defined network</td></tr><tr><td>SecGW</td><td>Security gateway</td></tr><tr><td>SLA</td><td>Service level agreement</td></tr><tr><td>SLS</td><td>Service level specification</td></tr><tr><td>SOC</td><td>Security operations center</td></tr><tr><td>SSL</td><td>Secure Sockets Layer</td></tr><tr><td>TLS</td><td>Transport Layer Security</td></tr><tr><td>TN</td><td>Transport network</td></tr><tr><td>UDM</td><td>Unified data management</td></tr><tr><td>UE</td><td>User equipment</td></tr><tr><td>uUpP</td><td>User plane</td></tr><tr><td>UPF</td><td>User Plane Function</td></tr><tr><td>URLLC</td><td>Ultra-reliable low-latency communication</td></tr><tr><td>V2I</td><td>Vehicle-to-infrastructure</td></tr><tr><td>V2N</td><td>Vehicle-to-network</td></tr><tr><td>v2p</td><td>Vehicle-to-pedestrian</td></tr><tr><td>vas</td><td>Vehicle-to-sensor</td></tr><tr><td>V2V</td><td>Vehicle-to-vehicle</td></tr><tr><td>V2X</td><td>Vehicle-to-everything</td></tr><tr><td>VM</td><td>Virtual machine</td></tr><tr><td>VNF</td><td>Virtual Network Function</td></tr><tr><td>VRAN</td><td>Virtual Radio Access Network</td></tr><tr><td>WAF</td><td>Web application firewall</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 733, 'parent\_id': 'f2c3ea4966d9b000241b1c038411bdf6', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '58da67b2804855963b62e804cbf8fd0c', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8f3f8cdf20b5d1b1dbcccb715257a872', 'text': 'Jason Longley and Pramod Nair, “Securing the 5G Core (5GC) and Evolved Packet Core (EPC) with Cisco Security,”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'parent\_id': '58da67b2804855963b62e804cbf8fd0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '27e4c578b971adf83eb7f167f463e0cd', 'text': 'https://www.cisco.com/c/en/us/solutions/collateral/service- provider/service-provider-security-solutions/white-paper-c11- 742166.pdf', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'parent\_id': '58da67b2804855963b62e804cbf8fd0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2fcb4f636065421eeced67773e1e1d45', 'text': 'Pramod Nair, “Securing 5G and Evolving Architectures,” Cisco Knowledge Networks, Cisco Public, September 17, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'parent\_id': '58da67b2804855963b62e804cbf8fd0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7ab793d07d89df6bf1e6ca80a7deb354', 'text': 'Pramod Nair, “Securing Your 5G Infrastructure to the Edge and Beyond,” Cisco Public, April 1, 2021', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'parent\_id': '58da67b2804855963b62e804cbf8fd0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3398efe098fe8ec0f8bd9233839ed366', 'text': '3GPP TS 33.501. V17.1.0, “Security architecture and procedures for 5G System.”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'parent\_id': '58da67b2804855963b62e804cbf8fd0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5c2258d5fcc6dcaca39fe4801ef0b0ce', 'text': '3GPP TS 28.530 V17.1.0, “Management and orchestration; Concepts, use cases and requirements”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'parent\_id': '58da67b2804855963b62e804cbf8fd0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36c909ac0ba1f09cd2eb0107ee2bc268', 'text': '3GPP TS 23.434 V17.1, “Service Enabler Architecture Layer for Verticals (SEAL)”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'parent\_id': '58da67b2804855963b62e804cbf8fd0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bafcfc87221f0176fab8c14c0e9cdab6', 'text': 'https://www.cisco.com/c/dam/en\_us/solutions/iot/demystifying-5g- industrial-iot.pdf', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'parent\_id': '58da67b2804855963b62e804cbf8fd0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b898265080cb15fffaf783ccf2f5e315', 'text': '5G Automotive Association, “C-V2X Use Cases and Service Level Requirements, Volume II,” https://5gaa.org', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'parent\_id': '58da67b2804855963b62e804cbf8fd0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f15ab5347c622d8976eb4eb536ba670c', 'text': '5GAA TR A-200094, https://5gaa.org', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'parent\_id': '58da67b2804855963b62e804cbf8fd0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3599a5a932f91027b41373ed7dc46042', 'text': 'https://www.ntia.gov/SBOM', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'parent\_id': '58da67b2804855963b62e804cbf8fd0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '01c254c04b91dd01b5db541bf92c422a', 'text': 'https://www.portshift.io/', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'parent\_id': '58da67b2804855963b62e804cbf8fd0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2e8d77d6c8f96e798d31f453290304c', 'text': 'https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Solution\_ Briefs/IA\_Networking\_Solution\_Brief.html', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 734, 'parent\_id': '58da67b2804855963b62e804cbf8fd0c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'text': 'Chapter 11. Prioritizing 5G Security Investments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '105c605b56745e1a44c90513e56b0fde', 'text': 'After reading this chapter, you should have a better understanding of the following topics:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4aa04bc4f27d864c55e9fb5fd151783e', 'text': '• The methods for creating a prioritized list of security capabilities and controls based on use cases, deployment models, and network deployment stages', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '244c6eb65055c421b87534c072253884', 'text': '• Summary of critical security controls for 5G deployment and their capabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b92fd0ed5e9b52c6a2dfe76c3e17a1f1', 'text': '• Mapping of security controls and its impact on 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '01449a9fc9b8b945f4220a4231bb8a62', 'text': 'While Chapter 10, “Building Pragmatic End-to-End 5G Security Architecture,” discussed security controls and capabilities required to secure 5G deployments, this chapter will take you through the considerations for prioritizing investments in securing your 5G network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8b845132d484f29b76b12fd8ebc010d7', 'text': 'This chapter will be of particular interest to the following individuals and teams from enterprise/5G service providers deploying 5GC and cybersecurity vendors planning product developments for 5G security use cases:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b52eddac97f3950266b3991409747b72', 'text': '• Security leaders within government organizations who need to prioritize investments in security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9bba16df180e12082ece79893a425f8a', 'text': '• Management consultants advising governments and service providers on 5G security investments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '27d0fc93e2cc5e3377c284a5e0804599', 'text': '• CSO and CTO teams from service providers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '38cf9b8fa881c78f3d674b8630946f0a', 'text': '• CSO and CTO teams from enterprise teams deploying NPN/private 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '73b1b8fe112543728306b8574dbcf2b0', 'text': '• Cybersecurity vendor security architects looking to secure 5GC deployments for their customers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6205463ef54d95353212d9bf6b85760f', 'text': '• Cybersecurity vendor product managers looking for use cases or features to enhance security products to cater for secure 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '571777dc440cac7457102cb338f60bb6', 'text': 'Normally, investments in service provider domains like Radio Access Node (RAN), Mobile Packet Core, and the like are necessary to improve coverage', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 735, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '194e9a2c184e4a1b9f3861b91772d884', 'text': 'and capacity, allowing better revenue generation. Unfortunately, in these investment scenarios, security is deprioritized because investments in security do not bring in revenue. Investments in security were usually limited to Internet-facing interfaces and consisted of deploying firewalls for inspection in roaming and interconnect as well as inspecting the user plane in the Gi interface and Carrier Grade Network Address Translation (CGNAT).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 736, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b9542fe01e3bf87798cf8166bebcb93d', 'text': '5G deployments will require a complete rethink of the way security is perceived due to the openness, disaggregation, and decomposition of the 3GPP and non-3GPP Network Functions (NFs). Furthermore, the use of open source software components to build 5G Cloud-Native Functions (CNFs) introduces higher risks, hence the need for required investments in securing your 5G deployments, be it for deploying a 5G public network or deploying private 5G/5G non-public networks (NPNs) by industry verticals.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 736, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2343be583e1aa90bee7d906480c634c6', 'text': 'This chapter discusses pragmatic 5G security investments, such as the bare- minimum security you need on Day 0 of a 5G deployment and then investing in security in a phase-by-phase manner and using a method to prioritize your security investments. The evolution of security capabilities and controls in your network, listed in Table 11-1, will depend on various criteria:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 736, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a026124525c7f1abc77da9dbe19df007', 'text': '• What deployment model (on-premises, public cloud, or hybrid) will you implement?', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 736, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '261c9e46d8fd719882d9409b4078a55b', 'text': '• What are the use cases you plan to fulfill?', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 736, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9517e9c864ba4e36568a1f526f64b88e', 'text': '• What type of 5G network architecture (Distributed RAN, O-RAN, VRAN, C-RAN) will you choose?', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 736, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1f2b21060fbf4aec564218aae1cfc1a5', 'text': '• What is the existing security posture of your network?', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 736, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '909f1e8c9121a222b7877bec20b09d64', 'text': 'Due to so many different variants and dependencies, it is almost impossible to have a single common priority list. The priority list of security investments provided in this chapter is based on the most commonly used deployment methods chosen by my customers. This priority list should help you create your own list, if needed.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 736, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '033a3f0cb2067a57a4185418ff9d2af3', 'text': 'Recommended practices dictate that you ensure that user and device security controls such as multifactor authentication (MFA), endpoint security, and DNS- based security are deployed even before the 5G network NFs and equipment are installed and configured for any of the deployment models. This is to ensure that you have commensurate security controls in your network to identify any malicious activity. If you do not have robust user and device', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 736, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '290d57979511946f499d68c741dffeef', 'text': 'security mechanisms implemented before the 5G network elements are deployed, any amount of security investment will not secure your network, as the malicious software might have already migrated from the user device to your network intentionally or unintentionally.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 737, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'edbaaec76d939e880ef34328019fd138', 'text': 'Security Controls Primary Security Capabilities Catered for by the Security Control Supply chain security Hardware and software supply chain security Secure development lifecycle process Software bill of materials Network access control for users and devices Granular user and device MFA for employees, vendors, contractors, and sub- access control contractors Role-based access control (RBAC) for users Device profiling User and device segmentation Securing remote user access Network access control for users and devices Endpoint protection DNS security for users and devices Granular visibility and immediate quarantine Secure interoperability Secure inter-public land mobile network (PLMN) roaming Secure roaming between private SG/NPN 5G networks and public service providers Enhanced E2E visibility, Visibility in control plane for inter[nd]Virtual Network monitoring, and anomaly Functions (VNFs) and Cloud-Native Network Functions detection (CNFs) communications NFVi visibility Detecting anomalies in encrypted traffic without decryption, including encrypted AP communication Anomaly detection in 5G network configurations Encrypted traffic malware detection (without decryption) Detection of rogue/fake eNB, gNB, MEC gateway Monitoring of cloud-deployed 5G CNFs Backward compatibility with 3G and 4G networks', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Security Controls</th><th>Primary Security Capabilities Catered for by the Security Control</th></tr></thead><tbody><tr><td>Supply chain security</td><td>Hardware and software supply chain security Secure development lifecycle process Software bill of materials Network access control for users and devices</td></tr><tr><td>Granular user and device access control</td><td>MFA for employees, vendors, contractors, and sub- contractors Role-based access control (RBAC) for users Device profiling User and device segmentation Securing remote user access Network access control for users and devices Endpoint protection DNS security for users and devices Granular visibility and immediate quarantine</td></tr><tr><td>Secure interoperability</td><td>Secure inter-public land mobile network (PLMN) roaming Secure roaming between private SG/NPN 5G networks and public service providers</td></tr><tr><td>Enhanced E2E visibility, monitoring, and anomaly detection</td><td>Visibility in control plane for inter[nd]Virtual Network Functions (VNFs) and Cloud-Native Network Functions (CNFs) communications NFVi visibility Detecting anomalies in encrypted traffic without decryption, including encrypted AP communication Anomaly detection in 5G network configurations Encrypted traffic malware detection (without decryption) Detection of rogue/fake eNB, gNB, MEC gateway Monitoring of cloud-deployed 5G CNFs Backward compatibility with 3G and 4G networks</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 738, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '858bb9cae0d155ea18c4bd7dba6c4dbd', 'text': 'Slice-level security Inter-slice security Intra-slice security Slice-based secondary authentication Slice-level visibility Secure orchestration and SDN layers Application-level security Secure software delivery Secure 5G CNF images Secure registry management Application-level policy enforcement User-to-application mapping (including containers) Establishing and following DevSecOps methodology Runtime Application Self-Protection (RASP) Static application software testing (SAST) Automated CI/CD Runtime security Container security (image scanning and so on) Application dependency mapping Microsegmentation Vulnerability management Compliance management Forensics Secure connectivity between CNFs API gateway Access and aggregation IPsec layer security MACsec with 802.1X Anti-DDoS Anti-DDoS (volumetric and application centric) Rate-limiting API requests using web application firewall API Security API authentication and authorization Encrypting the API using TLS/mTLS/IPsec Token-based authentication between 5G NFs Rate limiting Validation of verbose error messages', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Slice-level security</th><th>Inter-slice security Intra-slice security Slice-based secondary authentication Slice-level visibility Secure orchestration and SDN layers</th></tr></thead><tbody><tr><td>Application-level security</td><td>Secure software delivery Secure 5G CNF images Secure registry management Application-level policy enforcement User-to-application mapping (including containers) Establishing and following DevSecOps methodology Runtime Application Self-Protection (RASP) Static application software testing (SAST) Automated CI/CD Runtime security Container security (image scanning and so on) Application dependency mapping Microsegmentation Vulnerability management Compliance management Forensics Secure connectivity between CNFs API gateway</td></tr><tr><td>Access and aggregation layer security</td><td>IPsec MACsec with 802.1X</td></tr><tr><td>Anti-DDoS</td><td>Anti-DDoS (volumetric and application centric) Rate-limiting API requests using web application firewall</td></tr><tr><td>API Security</td><td>API authentication and authorization Encrypting the APl using TLS/mTLS/IPsec Token-based authentication between 5G NFs Rate limiting Validation of verbose error messages</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 739, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '29f9f28c95d4fc877d44704686fe91a6', 'text': 'Infrastructure security Security zoning controls Next-generation firewalling Anti-malware using sandboxing SSL decryption and inspection Rapid threat containment Application visibility and control Vulnerability management Vulnerability management of CNF deployed in multicloud and forensics stack Vulnerability management of VNFs and CNFs deployed on virtual machines (VMs) Vulnerability management of VNFs and CNFs deployed on bare metal (BM) Full lifecycle vulnerability scanning, including the build, ship, CI/CD pipeline, and runtime Forensics capability on VNFs and CNFs Automated capability of consolidating, de-duplicating, and correlating vulnerabilities Automatically identifying and fixing vulnerabilities in containers', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Infrastructure security controls</th><th>Security zoning Next-generation firewalling Anti-malware using sandboxing SSL decryption and inspection Rapid threat containment Application visibility and control</th></tr></thead><tbody><tr><td>Vulnerability management and forensics</td><td>Vulnerability management of CNF deployed in multicloud stack</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 740, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '39146bfa0276770c08ff1ba7032cb63a', 'text': 'Table 11-1 Summary of Critical 5G Security Controls and Its Capabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 740, 'parent\_id': '3c5ffccd55feddf91d20349a551cdfd1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'a8449e7eeda1ec8ca735b5922bc70fa9', 'text': 'Method of Prioritizing Security Controls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 740, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '75bd3be02c24f7fe9376f3241124ec7f', 'text': 'This section will discuss some concrete methods to prioritize the investments in security based on scenarios that consider different deployment methods and network types (public/non-public). The threat surfaces/risks and the priority of security controls to mitigate the risks are discussed using radar graphs. There are basically two key steps in determining the priority of the investments:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 740, 'parent\_id': 'a8449e7eeda1ec8ca735b5922bc70fa9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1ad528c0d1714f1c751ed55b5695f69f', 'text': 'Step 1 In this step, we will determine the level of threat surfaces/risks using a radar graph for two scenarios—a public network (service provider) scenario and a non-public network/private 5G (mostly used in industry verticals) scenario. Some of the key points that increase the criticality', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 740, 'parent\_id': 'a8449e7eeda1ec8ca735b5922bc70fa9', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8773eb9166c8e9a7e12131dab3036064', 'text': 'of the threats are related to possible attacks leading to service disruptions and thus revenue loss. By filling in the radar graph, we will determine the impact of each threat for each scenario and the stages of the scenarios. Here are the threats we will consider:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7194d1099b0413b65c13f3d01180587d', 'text': '• Supply chain vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd94fbd1161b27286990852bbea51909c', 'text': '• End-user device-based threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a3369059bd471f3b5451ca160f4f812', 'text': '• End-user-based threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7c0db2eb6d13498d3f3840897e9f4237', 'text': '• Infrastructure user-based threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '837c26eeee611f52763e5ba77c1f57a4', 'text': '• Infrastructure user-device-based threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dbd160381618687a6cc62c589b5bed32', 'text': '• API vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '75f897e37ac123f4b7eba5bd9f3717bf', 'text': '• MEC host vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ea02e167ff3b8b1ba2d50d874f0188a6', 'text': '• Public transport network vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd1bac05c923e6e2f7ccaaa56dcb8a790', 'text': '• CNF vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '541286306c4e7c0e1f26aa1c2c77c982', 'text': '• Threats from customer enterprise networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7d184eeab29bc5ea55b9fe8ce0008641', 'text': '• IoT device threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ea89a134bb8c1b826ef938ae15573697', 'text': '• C&C-based attacks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0dbd090c7dac47f157bd423a2e3e9631', 'text': '• Data exfiltration', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8c8d97798b5acb1cfde3ae25966dea10', 'text': 'Step 2 In this step, we will determine and prioritize the security controls to mitigate the threat surface using a radar graph. By filling in the spider graph, we will determine the priority of each of the security controls to mitigate the threats/risks. Some of the key points that help to improve the priority are related to multiple risk mitigation capabilities, such as the visibility and monitoring layer, which will help you tackle multiple threats with a single security control. Here are the key security controls and threat mitigation techniques detailed in Table 11-1:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '73f6c4377d3aba653fbfba95104ef9b5', 'text': '• Supply chain security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f340a46aaecdf462dbc673d34d7c0fae', 'text': '• Granular user access controls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '830d452fa226747194369464384bae41', 'text': '• Secure interoperability', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2252cebeebbeaca97a3820e96345d233', 'text': '• Application-level security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '14d74bb08cb31909c7ee0b0e02d7c6da', 'text': '• Vulnerability management and forensics', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 741, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '79fcf272d2889b974b34f642cd26aeb7', 'text': '• Slice-level security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 742, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2de50382aa5cc27d2971739be1d60c23', 'text': '• Enhanced visibility and monitoring', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 742, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '160c97d796af2ed3b389f667eeeb8afd', 'text': '• Secure access and aggregation', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 742, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6ffe98551f1e303bd9cd03fb443b870d', 'text': '• Anti-DDoS', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 742, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cef6abc42672713d49c3ff96ac6e28fb', 'text': '• API security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 742, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b2b69813f8987015e387ac5c04d8358c', 'text': '• Infrastructure security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 742, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a1acd4a6acbcc1c2f165ab6adf160a8a', 'text': 'Radar graphs are used throughout this chapter to provide you with a visual representation of the impacts of the threats and security controls. Figure 11-1 illustrates the split of the radar graph into varying levels of impact, from low to critical impact.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 742, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9487cbd149daf1d8f639839e1fed8dab', 'text': 'Threats / Securty controls with criical impact', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 743, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f77d4471753eebf4cd83146a059ee602', 'text': 'Threats / Securty controls with very high impact', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 743, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed2ee6738acce310faa901262ad3f7c7', 'text': 'Threats / Security controls with high impact', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 743, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '0cb17ce29eac853f147484b1fa3b69b1', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 743, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'b7181e50d06f6ec87ace337580ffdf36', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 743, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '73dfb2697fe4ec999556f4f094678df4', 'text': 'Threats / Securiy controls with medium impact', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 743, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '6dac2af241c546a955a4a1bd717a46cf', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 743, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '07882d500eee542a1b0d3ce398456334', 'text': 'Threats / Securiy controls with low impact', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 743, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'adf166602e83427148125e2504819340', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 743, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '0faaa9a3752ad0b90c59cfa8c536a947', 'text': '', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 743, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0b230bad7901b854b8ff0d2b749f170c', 'text': 'Figure 11-1 Key Split of Radar Graph into Varying Levels of Threats and Security Controls', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 743, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'baa5f1343ece58081fa8b7c9cba0f7ad', 'text': 'Table 11-2 shows an example of the mapping of threats/security controls and their impacts.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 743, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '6d341cac18c0c74eb2c968bdd0f00fad', 'text': 'Threats/Security Control R I I 2N I A A IR 2 I B 2 I I R I I 2 % v B - v E - ]', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Control Threats/Security</th><th></th><th></th><th></th><th>ol</th></tr></thead><tbody><tr><td></td><td></td><td></td><td></td><td>---</td></tr><tr><td></td><td></td><td></td><td></td><td>-----</td></tr><tr><td></td><td>IR</td><td>2</td><td>I</td><td>B</td></tr><tr><td></td><td>2</td><td>I</td><td>I</td><td>R</td></tr><tr><td>%;</td><td>I</td><td>I</td><td></td><td>2</td></tr><tr><td></td><td></td><td></td><td>|</td><td></td></tr><tr><td></td><td>v</td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td>B</td><td></td></tr><tr><td></td><td>-</td><td></td><td></td><td>v</td></tr><tr><td></td><td></td><td>[</td><td>|</td><td></td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 744, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1591331ef93d2601a3e4292dc6347ce1', 'text': 'Table 11-2 Mapping Threat/Security Controls and Impact', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 744, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '64e03d6179113410d84834f867700a07', 'text': 'Figure 11-2 illustrates the sample radar plot using the threat/security-control- to-impact mapping from Table 11-2.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 744, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '164efafba174840eb3b3373a2c7ee0bf', 'text': 'H G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 745, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e0236f4fd0741601bf534a4edfbc851b', 'text': 'Figure 11-2 Sample Radar Graph Plot Using Values from Table 11-2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 745, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4eea7b35ffbd200e6d1cff462dea9713', 'text': 'Figure 11-2 is an example of how the impact of the threats/security controls are plotted on the radar graph, giving you a visual representation to compare different deployment scenarios, such as public/non-public networks, along with the stages of deployment, such as initial/completion stage and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 745, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3030cb7c0c272f3dc6cffdd549c35658', 'text': 'Figure 11-3 illustrates how to interpret the graph.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 745, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '14d8202a2f0f03cbd3e4f0e6cfa57046', 'text': 'Q Medium Low Figure 11-3 Interpreting the Graphs Used in This Chapter', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 746, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '58ed043ea3ec6eb2bd7b457c753a8495', 'text': 'Figure 11-3 shows you the method used to interpret the radar graphs used in this chapter. It enables you to prioritize mitigating the most critical threats and prioritize investments on the right security controls. As an example, in Figure 11-3, the radar graph under the heading “Critical” has A, B, D, H, J, and M circled to indicate the specific threats/security controls that are critical. Note', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 746, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd964304c659efd880f38962fa9a5fd8b', 'text': 'that the graph for A, B, D, H, J, and M is plotted within the “critical” impact split of the radar graph.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3bf02afb3d1c159c4abfa1c35bfb6a59', 'text': 'The same graphical illustration is used to indicate the priority of the security controls to mitigate the threats and risks in the following sections of this chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3a1b338aab4d9179da72ecf6c057095e', 'text': "Let's look at some of the methods to prioritize the security controls based on various 5G network deployments.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'e666210a623e043edc185b5e695284de', 'text': 'Scenario 1', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f23282771162bd8f4ef82bba4cb0692', 'text': 'In this scenario, we will look at a service provider with a hybrid deployment model planning to implement three use cases: eMBB/VoNR, NSaaS, and IoT for consumers and enterprise customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'parent\_id': 'e666210a623e043edc185b5e695284de', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '51b3d1ac6802c157e2c3ec9c005d97d5', 'text': 'The details of Scenario 1 are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'parent\_id': 'e666210a623e043edc185b5e695284de', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '07ba0b67d19fdaa423ee198ea2a3330c', 'text': '• Network owner: Service provider', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'parent\_id': 'e666210a623e043edc185b5e695284de', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b586a16f4a70374a070964985d5390ad', 'text': '• Deployment model: Hybrid (on-premises and public cloud)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'parent\_id': 'e666210a623e043edc185b5e695284de', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9f5d43a7ad34652c6a823f7ef5a43f06', 'text': '• 5G architecture: Distributed RAN and Open RAN option 7-2x in some clusters', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'parent\_id': 'e666210a623e043edc185b5e695284de', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '44e975e89cab0a14f7a1105db2554ece', 'text': '• Primary use cases:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'parent\_id': 'e666210a623e043edc185b5e695284de', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f840e89927ed677ce2ec0b56ce5c7260', 'text': '• Stage 1: Enhanced mobile broadband (eMBB) and Voice over New Radio (VoNR) use cases for mobile subscribers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'parent\_id': 'e666210a623e043edc185b5e695284de', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9ce7dfb31206708a5fbf54d571300d1d', 'text': '• Stage 2: Network slice as a service (NSaaS) for enterprise customers and industry verticals', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'parent\_id': 'e666210a623e043edc185b5e695284de', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7d3119bcf3339dd9ee377a35d2fe9f62', 'text': '• Stage 3: IoT use cases for consumers and enterprise customers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'parent\_id': 'e666210a623e043edc185b5e695284de', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e32c4945b36d67b18fc797b209a6e928', 'text': 'The following steps will help you identify the priorities in investment toward the right security controls:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'parent\_id': 'e666210a623e043edc185b5e695284de', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '73d3b2ea8497cbe271ad4791cba923ac', 'text': 'Step 1 Identify the threats/threat modeling.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'parent\_id': 'e666210a623e043edc185b5e695284de', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a1f963dfd2d112ae79a2f679ba871a21', 'text': 'Step 2 Prioritize the key security controls to mitigate the threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'parent\_id': 'e666210a623e043edc185b5e695284de', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fd5aba2aecc2770367b684e21abc02a7', 'text': 'The sections that follow discuss Steps 1 and 2 in detail.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'parent\_id': 'e666210a623e043edc185b5e695284de', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'b3c3ed3edf3a330f39516929398876db', 'text': 'Step 1: Identifying the Threats/Threat Modeling', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 747, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1df97a361da4434a1eaf5c6962f1adf4', 'text': 'This section will take you through the threat modeling/identification of the key threats for the aforementioned three primary use cases, starting with the initial staging, implementation, and configuration onboarding. It then moves to Stage 1, which consists of voice and enhanced mobile broadband use cases (the primary use case many of service providers are planning to deploy), followed by network slicing and network slice as a service (NSaaS) in Stage 2, and then moving on to the advanced stage of providing customized IoT use cases for consumers and enterprise customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 748, 'parent\_id': 'b3c3ed3edf3a330f39516929398876db', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b0242af9f5daa462f3985aaf1fb60197', 'text': "Before we start with the specific use cases, let's have a look at the security controls required during the initial staging and onboarding of the network equipment and applications, which need to be implemented before the configuration and activation of the use cases.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 748, 'parent\_id': 'b3c3ed3edf3a330f39516929398876db', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '1f1f55f9845bba38210e514f34206f8a', 'text': 'Threats and Risks During Initial Staging and Onboarding', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 748, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b8384cd578724aef2aeaee8783e36408', 'text': 'Figure 11-4 illustrates the key threat surfaces and risks during initial deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 748, 'parent\_id': '1f1f55f9845bba38210e514f34206f8a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '94fc3a9533ce10a3647c41f1ca1e5ec1', 'text': 'Supply Chain based vulnerabilities Data Exfiltration End user device based DDoS attacks C&C based attacks End user based threats Infrastructure User loT device threats based threats Threats from Customer Enterprise Infrastructure User Device based threats Networks CNF Vulnerabilities API vulnerabilities Public Transport MEC Host Network vulnerabilities Vulnerabiliites', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 748, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b1b15eca1635ab20034a95e74c31b791', 'text': 'Figure 11-4 Key Threats Surfaces and Risks During Initial Deployment Phases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 748, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '440b87638b18fdbf0312fdff5e87131b', 'text': 'Figure 11-4 illustrates the key threat surfaces and risks during initial staging, onboarding, and implementation of your 5G network, even before any of the use cases are implemented for Scenario 1. The following areas are discussed:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 749, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '24b4552e09590b531e0cffb5135f651a', 'text': '• Hardware and software supply chain', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 749, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c6be6e534087d53296bbcb90546d064c', 'text': '• Risks from devices used by various vendors, subcontractors, and other users of your infrastructure to configure the 5G network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 749, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f9e68aac35f3d84256ec140ad378b64f', 'text': '• Risks from intentional and unintentional improper security configurations while configuring various physical and virtual components of the 5G network by users', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 749, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'de571b6cc413418b5d09e3ba50bc1e15', 'text': '• Centralized data center and MEC host hardware and software vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 749, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9f4ca914bfd34dfdd0fd0dfd1d4961e5', 'text': '• 5G Cloud-Native Function (CNF) image vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 749, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ce9951c5ff38cea9e0d88dfbba868269', 'text': 'Threats and Risks During eMBB and VoNR Use Case Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 749, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '46baf0b912088e81af9446598beaf17a', 'text': 'Figure 11-5 illustrates the key threat surfaces and risks when you implement the eMBB and VoNR use case.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 749, 'parent\_id': 'ce9951c5ff38cea9e0d88dfbba868269', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '20b5704fa152d21b8e1183aae1abe76e', 'text': 'Supply Chain based vulnerabilities End user device Data Exfiltration based DDoS attacks End user based C&C based attacks threats loT device threats Infrastructure User based threats Threats from Infrastructure User Customer Device based threats Enterprise Networks CNF Vulnerabilities API vulnerabilities Public Transport Network MEC Host vulnerabilities Vulnerabiliites', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 749, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b1721145a5885a64a130b6aeae93d1f1', 'text': 'Figure 11-5 Key Threat Surfaces and Risks While Deploying eMBB and VoNR', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 749, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1e1daca56a28044804692ba854e55c8b', 'text': 'The following threats and risks are critical when you deploy the eMBB and VoNR use case:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 750, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bbff3ac1fb0178cb93128b92ccf2263e', 'text': '• Hardware and software supply chain.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 750, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5dd49631925620e956d1258260f99193', 'text': '• Risks from devices used by various vendors, subcontractors, and other users of your infrastructure to configure the 5G network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 750, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '582dabf5226db0eb1d1c440285541a67', 'text': '• Risks from intentional and unintentional improper security configurations while configuring various physical and virtual components of the 5G network by users.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 750, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f79ffc9afb4af30ef94d6e5c3d8021a7', 'text': '• Risks due to improper configuration of the 3GPP and non-3GPP 5G CNFs for realization of eMBB use cases. The image download of 5G CNFs might be prone to inherent vulnerabilities due to improper checks being carried out by the vendor before uploading it to the container registry.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 750, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '31c4ea7f9964fda1cbc785a24ae4a92e', 'text': '• Centralized data center and MEC host hardware and software vulnerabilities.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 750, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e9d81180428be86ae0f60ef999001789', 'text': '• Risks due to improper API implementation and vulnerabilities of the API web server.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 750, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c3c8836c85508b5e32721a66567e292a', 'text': 'Threats and Risks While You Implement the NSaaS Offering', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 750, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '909f4199512a72646f31c9a9d2a68c0c', 'text': 'Figure 11-6 illustrates the key threat surfaces and risks when you implement the NSaaS use case.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 750, 'parent\_id': 'c3c8836c85508b5e32721a66567e292a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'be50e0f0aa530df6098e726c09115b8f', 'text': 'Supply Chain based vulnerabilities End user device Data Exfiltration based DDoS attacks C&C based attacks End user based threats Infrastructure User loT device threats based threats Threats from Infrastructure User Customer Device based Enterprise NW threats CNF Vulnerabilities API vulnerabilities Public Transport MEC Host NW Vulnerabiliites vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 751, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a6e9f4fc0d6248cdfc63b0273d0305bc', 'text': 'Figure 11-6 Key Threat Surfaces and Risks While Deploying the NSaaS Offering', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 751, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c5866ec09245ebbecc90ebcca103ac97', 'text': 'As illustrated in Figure 11-4, the key threat surfaces and risks during deployment of the NSaaS offering are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 751, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8f06f05f9e2ef8e88b79d96f6c3f3887', 'text': '• Hardware and software supply chain.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 751, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7dca1595303548c374fbdabd948945ae', 'text': '• Risks from intentional and unintentional improper security configurations while configuring various physical and virtual components of the 5G network for NSaaS deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 751, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4a7dd532632f79b1c53b6d99ed25373d', 'text': '• The image of the downloaded 5G CNFs might be prone to inherent vulnerabilities due to improper checks being carried out by the vendor before uploading it to the container registry.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 751, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1bb67838fad5adc200266c41c78f9f44', 'text': '• Improper API implementation in the management of the service layer in NSaaS deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 751, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d86539f03deea0e55f6ff8126482c14', 'text': '• DDoS and DoS threats from the devices of the other slices in the NSaaS deployment due to insufficient isolation between slice NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 751, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c188b4a1e9afdd91cd768b2427c9193e', 'text': '• Improper slice-level authentication for users and devices between NSaaS slices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 751, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '876dc066b1cd10674cb1eb1cc506f84c', 'text': 'Threats and Risks While You Implement IoT Use Cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 752, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6ed20c743ff952d34982f33353871b3b', 'text': 'Figure 11-7 illustrates the key threat surfaces and risks for when you implement IoT use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 752, 'parent\_id': '876dc066b1cd10674cb1eb1cc506f84c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '087f2057a0706d896b64e3a28c62a2c2', 'text': 'Supply Chain based vulnerabilities End user device Data Exfiltration ased DDoS attacks End user based C&C based attacks threats Infrastructure User loT device threats based threats Threats from Infrastructure User Customer... Device based threats CNF Vulnerabilities API vulnerabilities Public Transport NW MEC Host Vulnerabiliites vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 752, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dafde69468c73683276c73a16314a7ff', 'text': 'Figure 11-7 Key Threat Surfaces and Risks While Deploying IoT', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 752, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '08a9476ae57b6cf0293f2652462680b5', 'text': 'The key threat surfaces and risks during deployment of the massive IoT use case are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 752, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0344321e1d3c016637e1974d6f5478b0', 'text': '• Hardware and software supply chain', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 752, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd34beea1c4ef9cca9ced04496dc6088b', 'text': '• Risks from command and control (C&C) centers taking over the deployed IoT devices by exploiting their weak security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 752, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b5ca5a79c3f8d2daf466f897c381f497', 'text': '• Improper API implementation in the management of the IoT devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 752, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '66d438bf5b0c5aade7f7e3085f087aa0', 'text': '• DDoS threats from the IoT devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 752, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a97d438b9c25e94de99efadbc7a50de6', 'text': '• Improper slice-level authentications for users and devices between slices (eMBB, IoT, and other NSaaS slices)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 752, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2240a57e38880c3daf46fcbf5efc2545', 'text': 'Once we understand the threat model, key threats, and risks for deploying the use cases and creating new offerings, the investments in securing the 5G deployment can be prioritized as discussed in the following sections.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 753, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0e333c0a7109a456520bbcc8d78cb3ad', 'text': 'Step 2: Prioritize the Key Security Controls to Mitigate the Threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 753, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '932e3c474adaac3e468e8929faa85961', 'text': 'Step 1 identified the key threats in each of the three primary use cases. This section will determine the key security controls required to mitigate the threats identified in Step 1.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 753, 'parent\_id': '0e333c0a7109a456520bbcc8d78cb3ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd6ec45051bf08cacb452b3485fff8b08', 'text': 'This section starts by determining the key security controls you require for the initial staging and onboarding stages and then determines the key security controls for each of the use cases related to eMBB, NSaaS. and IoT deployment. The section also includes the priority list of security controls, if you plan to deploy eMBB, VoNR, NSaaS, and IoT all at once in different clusters of your network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 753, 'parent\_id': '0e333c0a7109a456520bbcc8d78cb3ad', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2c4e07083758daa62fcad927073337b2', 'text': 'Priority of Security Controls to Secure Initial Staging and Onboarding', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 753, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3b02f9ab1ed7c2a0e2cf3b22ddb0dd74', 'text': 'Figure 11-8 illustrates the security controls for securing the staging and onboarding phases of 5G deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 753, 'parent\_id': '2c4e07083758daa62fcad927073337b2', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'eed42633dbaf81276451c482e918d604', 'text': 'Supply Chain Security - HW & SW', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 754, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '43e24853865afda82ca5a5211e5fde4d', 'text': 'Supply Chain Security - HW & SW Infrastructure Granular User Access Controls Security Secure API security interoperability Anti-DDoS Application Level Security Vulnerability Access & Aggregation Management & Forensics Enhanced Visibility & Slice Level Security Monitoring', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 754, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4e271749663f2c81922b642ac837f9eb', 'text': 'Figure 11-8 Priority of Security Controls to Secure Initial Staging and Onboarding', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 754, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ba647ccb78a025ce2a19d15f88e19981', 'text': 'The key threat security controls for secure deployment during initial staging and onboarding are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 754, 'parent\_id': '4e271749663f2c81922b642ac837f9eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6083963542f4bc087927e0893b1094ed', 'text': '• Ensure you follow a robust process for supply chain security, including implementation of Secure Zero-Touch Provisioning (SZTP) procedures for the initial download of software in the access switches and routers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 754, 'parent\_id': '4e271749663f2c81922b642ac837f9eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da43895cb244ec4f6d0e2fcb8fc48e59', 'text': '• Granular access control for contractors, employees, part-time employees, and vendors during the initial configuration of applications and network equipment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 754, 'parent\_id': '4e271749663f2c81922b642ac837f9eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2ad020ee45204961ad968c7adb3b80bb', 'text': '• Application security, including securing inter-NF communications and applying microsegmentation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 754, 'parent\_id': '4e271749663f2c81922b642ac837f9eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3c5a0b040da8c7b9cf83de4663b207ee', 'text': '• Ensure API communications are secured and have the information of the TLS versions being used in the 5G network. TLS 1.3 is recommended because it is more robust than TLS 1.2.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 754, 'parent\_id': '4e271749663f2c81922b642ac837f9eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3658e611682d5a00673529cc6117bf57', 'text': '• Enhanced visibility, monitoring, and anomaly detection on the management and control plane, including encrypted traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 755, 'parent\_id': '4e271749663f2c81922b642ac837f9eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '85261bbbe97cb2f4524f6016c6729b4c', 'text': '• Create network security zones and anti-malware security controls within your data center and network infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 755, 'parent\_id': '4e271749663f2c81922b642ac837f9eb', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f5c087d237e79a717ba0c38dce511b49', 'text': 'Priority of Security Controls to Secure the Deployment of eMBB and VoNR Use Cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 755, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a437ee93a7f0af9cc2b9aa1f1f080850', 'text': 'Figure 11-9 illustrates the priority security controls for secure deployment of eMBB and VoNR use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 755, 'parent\_id': 'f5c087d237e79a717ba0c38dce511b49', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '35dda158eeb5bdd71b6a71bd1cc3b8be', 'text': 'Supply Chain Security - HW & SW Infrastructure Security Granular User Access Controls API security Secure interoperability Anti-DDoS Application Level Security Vulnerability Access & Aggregation Management & Forensics Enhanced Visibility Slice Level Security Monitoring', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 755, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2735804e3e8c0bdb136814529e25fbd1', 'text': 'Figure 11-9 Priority of Security Controls to Secure eMBB and VoNR Use Cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 755, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '974bd30468cbf8f920414974597ff6ac', 'text': 'The key threat security controls for secure deployment of eMBB and VoNR use cases are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 755, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '203297ff0162622ede4aa86fd7c74d3f', 'text': '• Ensure you follow a robust process for supply chain security, including hardware and software.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 755, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '87a51efda8056e6b33580a6f17431618', 'text': '• Granular access control to prevent unauthorized user access.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 756, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e488e06c7e6947bf95126171e8c3fcd7', 'text': '• Enhanced visibility, monitoring, and anomaly detection on the management and control plane, including encrypted traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 756, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b82a0efd6f534b9775fa822668cb4e38', 'text': '• Application security, including securing inter-NF communications and applying microsegmentation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 756, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4298de57b2d9879fc7bd54c4fb787afd', 'text': '• Create network security zones and anti-malware security controls within your data center and network infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 756, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0c650073ae8592489a0b35d4e40bd6d2', 'text': '• Secure xHaul and back-haul transport using IPsec', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 756, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2ee944896ba96c322c098e6016492617', 'text': 'Priority of Security Controls to Secure NSaaS Offering', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 756, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9bace469810933ec232efc13c110b56b', 'text': 'Figure 11-10 illustrates the priority of security controls to secure the NSaaS offering.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 756, 'parent\_id': '2ee944896ba96c322c098e6016492617', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'c49d8f8d35d2c10794470bbee6cdc24a', 'text': 'Supply Chain Security - HW & SW Infrastructure Granular User ccess Controls Security Secure API security interoperability Application Level Anti-DDoS Security Access & Vulnerability Management & Aggregation Forensics Enhanced Visibilit lice Level & Monitoring Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 756, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9dcbaae682f29b4c58945ec79d7d6a4d', 'text': 'Figure 11-10 Priority of Security Controls to Secure NSaaS Offerings', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 756, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '403af8573ac3fbe18751634b58ef0e75', 'text': 'The key security controls for a secure offering of NSaaS use cases are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 756, 'parent\_id': '9dcbaae682f29b4c58945ec79d7d6a4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ae2958558e70d709b47edaf616743e32', 'text': '• Ensure you follow a robust process for supply chain security, including hardware and software.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 757, 'parent\_id': '9dcbaae682f29b4c58945ec79d7d6a4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3937c4b5bb834f41c880622f9bab424b', 'text': '• Ensure granular access control in the management of the service layer in NSaaS to prevent unauthorized user access between communication service customers (CSCs).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 757, 'parent\_id': '9dcbaae682f29b4c58945ec79d7d6a4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dfe99dc3a2ae9fc32b69b6dc50985225', 'text': '• Implement enhanced visibility, monitoring, and anomaly detection on the management and control plane, including encrypted traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 757, 'parent\_id': '9dcbaae682f29b4c58945ec79d7d6a4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '98f94769a0dbe1bad151081505d0e08d', 'text': '• Secure interoperability between the NPN and public service providers and between the service provider and roaming partners.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 757, 'parent\_id': '9dcbaae682f29b4c58945ec79d7d6a4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f815bd6de588a7e1f8fda67fd60fb4e8', 'text': '• Implement application security, including securing inter-NF communication and applying microsegmentation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 757, 'parent\_id': '9dcbaae682f29b4c58945ec79d7d6a4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fad58ac2b367a87ba19cf564f5f2d04e', 'text': '• Apply slice-level secondary authentication mechanisms.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 757, 'parent\_id': '9dcbaae682f29b4c58945ec79d7d6a4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7937f4a7eb56683db12cf03e4e11cf1e', 'text': '• Create network security zones and anti-malware security controls within your data center and network infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 757, 'parent\_id': '9dcbaae682f29b4c58945ec79d7d6a4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd7c10f08f961fa29482f094372352ac2', 'text': '• Ensure secure API communication using API gateways or web application firewalls along with rate limiting. API security should also include granular authentication and authorization.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 757, 'parent\_id': '9dcbaae682f29b4c58945ec79d7d6a4d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '70e8eeafc5bf916c92e07f8512e8107a', 'text': 'Priority of Security Controls to Secure Deployment of IoT Use Cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 757, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '28d0dc9c79b7877f1c03c6bf76c3406d', 'text': 'Figure 11-11 illustrates the priority of security controls to secure the IoT use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 757, 'parent\_id': '70e8eeafc5bf916c92e07f8512e8107a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '84540c42c9768a32a8b0d038e79e66d0', 'text': 'Supply Chain Security - HW & Sw Granular User & Infrastructure Device Access Security Controls Secure API security interoperability Anti-DDoS Application Level Security Vulnerability Access & Aggregation Management & Forensics Enhanced Visibili & Monitoring Slice Level Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 758, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd13dd5b1395075c14acee819de5c98a0', 'text': 'Figure 11-11 Priority of Security Controls to Secure IoT Deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 758, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6b17d7f63c831d5643a8e1cf225a9e87', 'text': 'The key threat security controls for secure IoT use cases are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 758, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9d9c4be895a8060f60ca96750d76b596', 'text': '• Ensure you follow robust process for supply chain security, including hardware and software of IoT devices and IoT network gateways.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 758, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cd7f78b6edee4563398d49619e1f79f1', 'text': '• Implement granular access control to prevent unauthorized user access.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 758, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a2cacf7ffc82ccc376de88f949e13463', 'text': '• Implement granular slice-level device authentication.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 758, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4df854e2e7fba4a2a09393bf8464bfa8', 'text': '• Implement enhanced visibility, monitoring, and anomaly detection on the management and control plane, including encrypted traffic of the IoT network slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 758, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fa1079511c1b58748ad9890533a0b586', 'text': '• Implement application security, including securing inter-NF communications and applying microsegmentation and application-level security controls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 758, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd43343100fb2b64b37f7b5bbdb8de018', 'text': '• Create network security zones and anti-malware security controls within your data center and network infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 758, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7985b98dfd009115d5faedb7dbd58383', 'text': '• Implement DDoS protection against the IoT devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 758, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '91c9d56877fe6bc3fbce26d1c61df138', 'text': 'Priority of Security Controls Catering for All Three Use Cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 759, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '76e4abc251039d60e327c603fa37a62c', 'text': 'If you plan to deploy all the three use cases together in the same cluster or different parts of the network, the following process will help you determine the key security controls required to ensure secure rollout of all three use cases —eMBB and VoNR, NSaaS, and IoT—together in your network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 759, 'parent\_id': '91c9d56877fe6bc3fbce26d1c61df138', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0e342156aea521356f995a9735b85cdb', 'text': 'Table 11-3 indicates the priority of the security controls for each of the use cases and then helps you determine the priority of the security controls when all three use cases are deployed together. This table also allows you to understand the highest priority of each of the use cases and then select that priority for the respective security control.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 759, 'parent\_id': '91c9d56877fe6bc3fbce26d1c61df138', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fc30b8cb2af95bd963a28b1da8676d79', 'text': "As an example, looking at the Anti-DDoS entry in Table 11-3, you can see it's a “critical” security control for IoT use case and is a “high” and “very high” security control for eMBB/VoNR and NSaaS use cases, respectively. If you plan to deploy all three use cases, the highest security priority for the use case is selected. In this case, the anti-DDoS security control would be a “critical” security control.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 759, 'parent\_id': '91c9d56877fe6bc3fbce26d1c61df138', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2a989e640933c6723d1236596778b494', 'text': 'If you are interested in only deploying eMBB/VoNR and NSaaS use cases, the priority of the anti-DDoS security control would be “very high” instead of “critical,” as “very high” is the highest priority when deploying the eMBB/VoNR and NSaaS use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 759, 'parent\_id': '91c9d56877fe6bc3fbce26d1c61df138', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '6ba52815347eb154b4f1194c7aff364d', 'text': 'All Three Use eMBB and NSaaS IoT VoNR Cases Deployed Together Security Control Priority/Impact Priority/Impact Priority/Impact Priority/Impact Supply Chain Critical Critical Critical Critical Security [nd] HW and SW Granular User Critical Critical Critical Critical Access Controls Secure Critical Critical High Critical Interoperability Application- Level Security Critical Critical Critical Critical Vulnerability Management Very High Very High Very High Very High and Forensics Slice-Level High Critical Critical Critical Security Enhanced Critical Critical Critical Critical Visibility and Monitoring Access and High Very High Very High Very High Aggregation Anti-DDoS Critical Critical High Very High Critical Critical Critical API Security Very High Infrastructure Critical Critical Critical Critical Security', 'metadata': {'text\_as\_html': '<table><thead><tr><th></th><th>eMBB and VoNR</th><th>NSaaS</th><th>IoT</th><th>All Three Use Cases Deployed Together</th></tr></thead><tbody><tr><td>Security Control</td><td>Priority/Impact</td><td>Priority/Impact</td><td>Priority/Impact</td><td>Priority/Impact</td></tr><tr><td>Supply Chain Security [nd] HW and SW</td><td>Critical</td><td>Critical</td><td>Critical</td><td>Critical</td></tr><tr><td>Granular User Access Controls</td><td>Critical</td><td>Critical</td><td>Critical</td><td>Critical</td></tr><tr><td>Secure Interoperability</td><td>Critical</td><td>Critical</td><td>High</td><td>Critical</td></tr><tr><td>Application- Level Security</td><td>Critical</td><td>Critical</td><td>Critical</td><td>Critical</td></tr><tr><td>Vulnerability Management and Forensics</td><td>Very High</td><td>Very High</td><td>Very High</td><td>Very High</td></tr><tr><td>Slice-Level Security</td><td>High</td><td>Critical</td><td>Critical</td><td>Critical</td></tr><tr><td>Enhanced Visibility and Monitoring</td><td>Critical</td><td>Critical</td><td>Critical</td><td>Critical</td></tr><tr><td>Access and Aggregation</td><td>High</td><td>Very High</td><td>Very High</td><td>Very High</td></tr><tr><td>Anti-DDoS</td><td>High</td><td>Very High</td><td>Critical</td><td>Critical</td></tr><tr><td>API Security</td><td>Very High</td><td>Critical</td><td>Critical</td><td>Critical</td></tr><tr><td>Infrastructure Security</td><td>Critical</td><td>Critical</td><td>Critical</td><td>Critical</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 760, 'parent\_id': '91c9d56877fe6bc3fbce26d1c61df138', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5a9805ee1ee8d9c6028404de494ad660', 'text': 'Table 11-3 Security Control Priorities for All Use Cases in Scenario 1', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 761, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c7581883f9aecbac13d92a28a6785e5a', 'text': 'Figure 11-12 illustrates the priority of security controls to secure the eMBB, VoNR, NSaaS, and IoT use cases.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 761, 'parent\_id': '5a9805ee1ee8d9c6028404de494ad660', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'ffe71d02352bd4803f43bf47f90bf841', 'text': 'Supply Chain Security - HW & Sw Granular User & Infrastructure Device Access Security Controls Secure API security interoperability Application Level Anti-DDoS Security Access & Vulnerability Management & Aggregation Forensics Enhanced Visibilit Slice Level Security & Monitoring', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 761, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '245a30e90255f57fc20f49399d1137d9', 'text': 'Figure 11-12 Priority of Security Controls to Secure Deployments of All Three Use Cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 761, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd21026e02b25446253d67ec73ac39fd6', 'text': 'The key threat security controls for securing all three use cases are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 761, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3729e58eebe6350b9d2af076f82a90b1', 'text': '• Ensure you follow a robust process for supply chain security, including hardware and software.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 761, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '636c34b70425e4419324d19288cdb671', 'text': '• Implement granular access control to prevent unauthorized user access.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 761, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0b7f6db3a6cbfd0099753802050ec649', 'text': '• Ensure enhanced visibility, monitoring, and anomaly detection on the management and control plane, including encrypted traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 761, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dbbac93f8dfc6f85bd041ebd4186bfa7', 'text': '• Implement application security, including securing inter-NF communications and applying microsegmentation.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 761, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fe69eaa7365326aeef1fda1cfa56e8c8', 'text': '• Secure API communication using API gateways or web application firewalls along with rate limiting. API security should also include', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 761, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4969a5c6062801c944c636bcad52402a', 'text': 'granular authentication and authorization. Also, ensure secure API communication between the orchestration and SDN layers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 762, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4dfdc1ffd844054508577ce61a1cfa0e', 'text': '• Create network security zones and anti-malware security controls within your data center and network infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 762, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '765baee724b83c612adc409685a266a3', 'text': '• Implement DDoS protection against the IoT devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 762, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '46c8763a8b6da91d86fc8e05e9027e3a', 'text': 'Summary of Priority Security Controls for Scenario 1', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 762, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f2adc1b1e9d40fb1ef284516ad4c5efb', 'text': 'Table 11-4 illustrates the priority of security controls to secure Scenario 1. The Notes column in the Table 11-4 explains the reasoning and logic for determining the priority for the security controls catering for all three use cases. The priority will change, as mentioned in the beginning of the section “Priority of Security Controls for All Three Use Cases,” based on the number of use cases you plan to deploy in your network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 762, 'parent\_id': '46c8763a8b6da91d86fc8e05e9027e3a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '0fd07e3fed2cedf512fd6e8e191fd350', 'text': 'Notes Security Control Priority of Mapping Investment Investment Priority to Deployment Stages Supply Chain Critical Required from Mandatory to be verified and Security [nd] HW initial validated during initial and SW deployment and deployment and throughout the staging of operation of live networks. equipment and CNFs Granular User Critical Required from Mandatory during initial Access Controls initial deployment and throughout the deployment and operation of live networks. staging of equipment and CNFs Secure Critical Required before Mandatory once the network is Interoperability roaming is live for roaming use cases and implemented interconnect between NPN and and for NPN public networks as well as for interconnect NSaaS deployments. Not required with public during initial network networks implementation stage. Application-Level Critical Required from Mandatory to be verified and Security initial validated during initial deployment and deployment and throughout the staging of operation of live networks. equipment and CNFs Vulnerability Very High Required during Mandatory to be deployed for live Management and initial stages networks. Forensics but less of a priority than access control, supply chain monitoring, and API security.', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Security Control</th><th>Priority of Investment</th><th>Mapping Investment Priority to Deployment Stages</th><th>Notes</th></tr></thead><tbody><tr><td>Supply Chain Security [nd] HW and SW</td><td>Critical</td><td>Required from initial deployment and staging of equipment and CNFs</td><td>Mandatory to be verified and validated during initial deployment and throughout the operation of live networks.</td></tr><tr><td>Granular User Access Controls</td><td>Critical</td><td>Required from initial deployment and staging of equipment and CNFs</td><td>Mandatory during initial deployment and throughout the operation of live networks.</td></tr><tr><td>Secure Interoperability</td><td>Critical</td><td>Required before roaming is implemented and for NPN interconnect with public networks</td><td>Mandatory once the network is live for roaming use cases and interconnect between NPN and public networks as well as for NSaaS deployments. Not required during initial network implementation stage.</td></tr><tr><td>Application-Level Security</td><td>Critical</td><td>Required from initial deployment and staging of equipment and CNFs</td><td>Mandatory to be verified and validated during initial deployment and throughout the operation of live networks.</td></tr><tr><td>Vulnerability Management and Forensics</td><td>Very High</td><td>Required during initial stages but less of a priority than access control, supply chain monitoring, and API security.</td><td>Mandatory to be deployed for live networks.</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 763, 'parent\_id': '46c8763a8b6da91d86fc8e05e9027e3a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '3e21a973ae07bcbb7968478c3a8f27d9', 'text': "Slice-Level Critical Required before Mandatory to be deployed when Security network slicing slicing is implemented in your is implemented network. If your network doesn't use slicing in the initial years of deployment, you can plan it closer to deployment of network slicing. Enhanced Critical Required from Mandatory during initial Visibility and initial deployment and throughout the Monitoring deployment and operation of live networks. staging of equipment and CNFs Access and Very High Required if Mandatory if you are using a Aggregation public network public network for back-hauling. is used in back If you are using your own back- haul/xHaul and haul transport network, you can if country implement these security controls regulators have when you have integration points advised using it with third-party back-haul as a mandatory transport providers. Some security control countries have a mandatory requirement of using a security gateway in the back haul/xHaul defined by the country's regulator. Anti-DDoS Critical Required once Mandatory once the network is the network is live, primarily in Internet-facing live interfaces. Not required during initial network implementation stage. API Security Critical Required from Mandatory during initial initial deployment and throughout the deployment and operation of live networks. staging of equipment and CNFs Infrastructure Critical Required from Mandatory during initial Security initial deployment and throughout the deployment and operation of live networks. for providing segmentation of control plane and user plane traffic", 'metadata': {'text\_as\_html': "<table><thead><tr><th>Slice-Level Security</th><th>Critical</th><th>Required before network slicing is implemented</th><th>Mandatory to be deployed when slicing is implemented in your network. If your network doesn't use slicing in the initial years of deployment, you can plan it closer to deployment of network slicing.</th></tr></thead><tbody><tr><td>Enhanced Visibility and Monitoring</td><td>Critical</td><td>Required from initial deployment and staging of equipment and CNFs</td><td>Mandatory during initial deployment and throughout the operation of live networks.</td></tr><tr><td>Access and Aggregation</td><td>Very High</td><td>Required if public network is used in back haul/xHaul and if country regulators have advised using it as a mandatory security control</td><td>Mandatory if you are using a public network for back-hauling. If you are using your own back- haul transport network, you can implement these security controls when you have integration points with third-party back-haul transport providers. Some countries have a mandatory requirement of using a security gateway in the back haul/xHaul defined by the country's regulator.</td></tr><tr><td>Anti-DDoS</td><td>Critical</td><td>Required once the network is live</td><td>Mandatory once the network is live, primarily in Internet-facing interfaces. Not required during initial network implementation stage.</td></tr><tr><td>API Security</td><td>Critical</td><td>Required from initial deployment and staging of equipment and CNFs</td><td>Mandatory during initial deployment and throughout the operation of live networks.</td></tr><tr><td>Infrastructure Security</td><td>Critical</td><td>Required from initial deployment and for providing segmentation of control plane and user plane traffic</td><td>Mandatory during initial deployment and throughout the operation of live networks.</td></tr></tbody></table>", 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 764, 'parent\_id': '46c8763a8b6da91d86fc8e05e9027e3a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Header', 'element\_id': '81dd366ff02b9f7bdf73e353cbeaac24', 'text': 'Table 11-4 Summary of Investment Priority for Scenario 1', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0c6064b4ab9a0d130a70f3719de03201', 'text': 'Scenario 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '81dd366ff02b9f7bdf73e353cbeaac24', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9c2373476b2af93a805a1f4f273f25b8', 'text': 'In the previous section, we took the service provider deployment scenario and mainly focused on three use cases and determined the priority of the security controls based on the use cases you plan to deploy.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '0c6064b4ab9a0d130a70f3719de03201', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c88900e9a039ad20682b6141f42f2420', 'text': 'This section will take you through Scenario 2, which is focused on different stages of non-public network (NPN) deployment, beginning from standalone NPN (SNPN) deployment and then moving toward public network integrated NPN (PNI-NPN). This section also identifies the priority of the security control if you have both SNPN and PNI-NPN deployments in your network. This could be the case if you decide to have part of your industry vertical network air-gapped and choose the SNPN model and decide to have the other part to be more open and integrated to a public network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '0c6064b4ab9a0d130a70f3719de03201', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5d2ef902dd398e89f2afa585f5e784dd', 'text': 'By using the radar graph, you can further identify the key threats and determine the key security controls, ensuring that you have the security agility to secure your network from the changing threat landscape.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '0c6064b4ab9a0d130a70f3719de03201', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36cc27118a12ebc613de8343ef78e112', 'text': 'Here are the details of Scenario 2:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '0c6064b4ab9a0d130a70f3719de03201', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fc9813215fc48862f88ff396e9be1bd9', 'text': '• Network owner: Enterprise/industry vertical', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '0c6064b4ab9a0d130a70f3719de03201', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f2bf499ce0613c4a8e92fc6ba098361e', 'text': '• Industry Vertical type: Smart manufacturing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '0c6064b4ab9a0d130a70f3719de03201', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fa2011308cc91c237768a96a9a87fb5b', 'text': '• Deployment model: Hybrid (on-premises and public cloud)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '0c6064b4ab9a0d130a70f3719de03201', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7d528a101a4f20675057bcf2f95b5ee2', 'text': '• 5G Architecture: Distributed RAN', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '0c6064b4ab9a0d130a70f3719de03201', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0990c23ccaac8613175f1b38b16deeb4', 'text': '• Primary use cases deployed in stages:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '0c6064b4ab9a0d130a70f3719de03201', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a875aefce8db69a49021ba8b5e9fe981', 'text': '• Stage 1: Standalone non-public network (SNPN) – IoT/IIoT use case for URLLC use case', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '0c6064b4ab9a0d130a70f3719de03201', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'da885faf0ccbb07a8bfa91043f979e17', 'text': '• Stage 2: PNI-NPN integration with a communication service provider (CSP)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '0c6064b4ab9a0d130a70f3719de03201', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '70826e02fb358b9ec05706505603d2ca', 'text': 'Details of deployment in Stage 1:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '81dd366ff02b9f7bdf73e353cbeaac24', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd1a82c67467e683571e46779073806de', 'text': '• 5G control plane (CP) and user plane (UP) CNFs and equipment deployed within on-premises/private DC of smart manufacturing', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '70826e02fb358b9ec05706505603d2ca', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c8a1269437abc9d00e121eab1e4c1252', 'text': '• IoT and IIoT devices and sensors to be deployed and integrated with the 5G infrastructure', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 765, 'parent\_id': '70826e02fb358b9ec05706505603d2ca', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '0afbd3535d483329cea98d4ae3717441', 'text': 'Details of deployment details in Stage 2:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 766, 'parent\_id': '81dd366ff02b9f7bdf73e353cbeaac24', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd6ce445b31aac1ba77d48e87223533c0', 'text': '• Integration with public network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 766, 'parent\_id': '0afbd3535d483329cea98d4ae3717441', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '584becc750920e5d485002de57af8d50', 'text': '• Integration with communication service provider (CSP)/public service provider', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 766, 'parent\_id': '0afbd3535d483329cea98d4ae3717441', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b57d025e2bf78b21cc69c9c8d4ce25ea', 'text': 'The following steps will help you identify the priorities in investment toward the right security controls:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 766, 'parent\_id': '0afbd3535d483329cea98d4ae3717441', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '73968af2ae132c4a88b4403ef334ae2d', 'text': 'Step 1 Identify the threats/threat modelling', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 766, 'parent\_id': '0afbd3535d483329cea98d4ae3717441', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ccec05415b0cc21de56f965fb792a79b', 'text': 'Step 2 Prioritize the key security controls to mitigate the threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 766, 'parent\_id': '0afbd3535d483329cea98d4ae3717441', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ddcc6a1de21155caa49c902bbfe0085a', 'text': 'The sections that follow discuss Steps 1 and 2 in detail.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 766, 'parent\_id': '0afbd3535d483329cea98d4ae3717441', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3dde58f50dcc63883b4670d47544c83b', 'text': 'Step 1: Identifying the Threats/Threat Modeling', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 766, 'parent\_id': '81dd366ff02b9f7bdf73e353cbeaac24', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd00d373059d3bc91e4ae864a47cc1520', 'text': 'This section will take you through the threat modeling/identification for Stage 1, starting with the initial staging, implementation, and configuration onboarding. It then moves to Stage 1, which consists of voice and enhanced mobile broadband use cases, which is the primary use case that many of the service providers are planning to deploy, followed by NSaaS in Stage 2, and then moving to the advanced stage of providing customized IoT use cases for consumers and enterprise customers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 766, 'parent\_id': '3dde58f50dcc63883b4670d47544c83b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8c8840c2acfe8ce5de760576233364cf', 'text': 'Threats and Risks During Initial Staging and Onboarding', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 766, 'parent\_id': '81dd366ff02b9f7bdf73e353cbeaac24', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1dc5ac4707cfeb97b08b873dfcb44f36', 'text': 'Figure 11-13 illustrates the threat surfaces and risks during the initial deployment before Stage 1 goes live.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 766, 'parent\_id': '8c8840c2acfe8ce5de760576233364cf', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'cc9e8a79f1a5347b5e5530659e1fd23d', 'text': 'Supply Chain based vulnerabilities End user device Data Exfiltration based threats End user based C&C based attacks threats Infrastructure User loT device threats based threats Threats from Infrastructure User Customer Enterprise Device based Networks threats CNF Vulnerabilities API vulnerabilities Public Transport MEC Host Network Vulnerabiliites vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 767, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2249524332b05dcc749b1adb31fa4c64', 'text': 'Figure 11-13 Key Risks and Threat Surfaces During Initial Deployment Phases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 767, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0d23051658b13998b97edd90dbf49d1a', 'text': 'Here are the key threat surfaces and risks during initial staging, onboarding, and implementation of your NPN 5G network even before any of the use cases are implemented for Scenario 2:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 767, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ebff983e169a36f21de766ad1b46047f', 'text': '• Hardware and software supply chain, including hardware and software for 5G 3GPP and non-3GPP components', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 767, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ca77dd24e1559f8618473ee491fe1c01', 'text': '• Risks due to improper segmentation between your IT and OT/IIoT network, leading to threats migrating from IT to the OT and IIoT environment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 767, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6badc06f49caf88f37a21f19e41b4b89', 'text': '• Risks from devices used by various vendors, subcontractors, and other users of the infrastructure to configure your NPN 5G network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 767, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4d9a2e14480a6fea0285aa3ae2149172', 'text': '• Risks from intentional and unintentional improper security configurations while configuring various physical and virtual components of the 5G network by users', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 767, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '799699bbab6bd3452c71570b8e3ca7b9', 'text': '• 5G Cloud-Native Function (CNF) image vulnerabilities for 3GPP and non- 3GPP NFs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 768, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd84ca0ff281b704c830183b4ba858d1a', 'text': '• Centralized data center and MEC host hardware and software vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 768, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '265b42fbfff51a7ad020023c5555d753', 'text': 'Threats and Risks for Stage 1', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 768, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '30e096d1df36b3b75cc89ad68f056003', 'text': 'Figure 11-14 illustrates the threat surfaces and risks for Stage 1.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 768, 'parent\_id': '265b42fbfff51a7ad020023c5555d753', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '359f6588443fdb42d9184d023d56a156', 'text': 'Supply Chain based vulnerabilities End user device Data Exfiltration based threats End user based C&C based attacks threats Infrastructure User loT device threats based threats Threats from Infrastructure User Customer Device based Enterprise Networks threats CNF Vulnerabilities API vulnerabilities Public Transport Network MEC Host Vulnerabiliites vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 768, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '83b3a297e23c53f54b484553c72b4b5c', 'text': 'Figure 11-14 Key Risks and Threats Surfaces During Stage 1', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 768, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ff071298c3ebf313fc127b4545342566', 'text': 'Here are the key threat surfaces and risks that are critical during deployment of Stage 1:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 768, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7e6d084c9f09bec4cc0286f95912554a', 'text': '• Hardware and software supply chain, including hardware and software for 5G 3GPP and non-3GPP components', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 768, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0907cc8a271046e34762f9a835e3f702', 'text': '• Risks due to improper segmentation between your IT and OT/IIoT network, leading to threats migrating from IT to the OT and IIoT environment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 768, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6cc80203cdfac3dbe6fc5a484a071daf', 'text': '• Risks from devices used by various vendors, subcontractors, and other users of the infrastructure to configure your NPN 5G network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 769, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2f92323f6cc1a06f34dcb6d34d7f11d4', 'text': '• Risks from intentional and unintentional improper security configurations while configuring various physical and virtual components of the 5G network by users', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 769, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8439fcaa54343b197a1c9ba22de58f15', 'text': '• Risks due to improper implementation of the API and vulnerabilities within the API itself', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 769, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1d0013acd1a33227f0b72d72f51860f9', 'text': '• 5G CNF image vulnerabilities for 3GPP and non-3GPP NFs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 769, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4e82150581b5e6c76e4d5c04bf8ad980', 'text': '• Centralized data center and MEC host hardware and software vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 769, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '3415ca8898f6676fff77c7c50ca32177', 'text': 'Threats and Risks for Stage 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 769, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9bad4237da7229335015ffe3caaca655', 'text': 'Implementing Stage 2/PNI-NPN will depend on the architecture and use case you plan to implement. Depending on use case, you might not deploy Stage 1/SNPN and might implement only Stage 2/PNI-NPN. In some use cases, you might deploy only SNPN or Stage 1 only. Figure 11-15 illustrates the threat surfaces and risks for Stage 2.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 769, 'parent\_id': '3415ca8898f6676fff77c7c50ca32177', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '4e1ce20aba8c36aff69b828eb0060fe0', 'text': 'Supply Chain based vulnerabilities End user device Data Exfiltration based threats End user based C&C based attacks threats Infrastructure User loT device threats based threats Threats from Infrastructure User Customer Enterprise Device based threats Networks CNF Vulnerabilities API vulnerabilities Public Transport MEC Host Network vulnerabilities Vulnerabiliites', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 770, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8f31c52fa085c4c51cccffc4ec5b1583', 'text': 'Figure 11-15 Key Risks and Threats Surfaces During Stage 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 770, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f791b4f33a8150deae085d9dcdf6bb16', 'text': 'Here are the key threat surfaces and risks during deployment of Stage 2:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 770, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '45fd383c8b71d9b0555991397b77990a', 'text': '• Hardware and software supply chain, including hardware and software for 5G 3GPP and non-3GPP components', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 770, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8345592d03b6e37459a53bc4704b3332', 'text': '• Data exfiltration due to integration with external networks such as public service provider and data networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 770, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0cdf469dcfa60429cdb550c7682e2ae1', 'text': '• C&C attacks by exploiting vulnerabilities in an IoT/IIoT device within the smart manufacturing unit', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 770, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fbb282b0e6351277c1010d7e651075df', 'text': '• Man-in-the-middle (MitM) attacks due to exposure of the NPN network to the public network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 770, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67d3f57b5de62c0f1f392d7829d5e667', 'text': '• Risks due to improper segmentation between your IT and OT/IIoT network, leading to threats migrating from IT to the OT and IIoT environment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 770, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f6e70841f6ade1cd57317c752458e416', 'text': '• Risks from devices used by various vendors, subcontractors, and other users of the infrastructure to configure your NPN 5G network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 771, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e5264a00a446f0b3ba738b487c159c2f', 'text': '• Risks from intentional and unintentional improper security configurations while configuring various physical and virtual components of the 5G network by users', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 771, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1127c6f45c87923ddabf494f227091c7', 'text': '• 5G CNF image vulnerabilities for 3GPP and non-3GPP NFs', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 771, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5a9371b5d217bbc050ffe49d2fd63abe', 'text': '• Centralized data center and MEC host hardware and software vulnerabilities', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 771, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5b248ab36679042d2e5ed90d9684567b', 'text': 'Step 1 so far has identified the key threats and the impacts for each of the threats in Stage 1 and Stage 2. The next step (Step 2) is to determine the security controls required to mitigate the threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 771, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '65a45673c1215dc884f7e90570191691', 'text': 'Step 2: Prioritize the Key Security Controls to Mitigate the Threats', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 771, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2f11bcb9ae6ec83df17943e28654a3a2', 'text': 'Step 1 identified the key threats for Stage 1 and Stage 2 for NPN deployments. This section will determine the key security controls required to mitigate the threats identified in Step 1.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 771, 'parent\_id': '65a45673c1215dc884f7e90570191691', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4966258e847527073d09296377a769d4', 'text': 'This section will start by determining the key security controls you require for the initial staging and onboarding stages and then determine the key security controls for Stage 1 and Stage 2. The section also includes the priority list of security controls, if you plan to deploy both Stage 1 and Stage 2 together in your network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 771, 'parent\_id': '65a45673c1215dc884f7e90570191691', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '87a34881b932281f05660924d86eddac', 'text': 'Priority Security Controls During Staging and Onboarding', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 771, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2d000c8e8f47461e1f8f563d722394de', 'text': 'Figure 11-16 illustrates the priority of security controls to secure the initial staging, onboarding, and implementation phase before Stage 1 goes live.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 771, 'parent\_id': '87a34881b932281f05660924d86eddac', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '5a1730aded09b21f6557f2b8653c6535', 'text': 'Supply Chain Security - HW & SW OT & Infrastructure Granular User Security Access Controls Secure API security interoperability Anti-DDoS Application Level Security Access & Vulnerability Management & Aggregation Forensics Enhanced Visibility Slice Level Security Monitoring', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 772, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3837adb08c45704e29affb6fdfe0247e', 'text': 'Figure 11-16 Priority of Security Controls to Secure Initial Deployment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 772, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a85b57ed5361a028ec1ad6fc8c92d47', 'text': 'Here are the key threat security controls for securing the initial staging, onboarding, and implementation phase before Stage 1 goes live:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 772, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '26ef5ad2ac64e3fcc1e2ce79d481c9da', 'text': '• Ensure you follow a robust process for supply chain security, including hardware and software of IIoT/IoT devices and IIoT network gateways.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 772, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ed34fed91acfdf0ab3f6e462d4f657f0', 'text': '• Implement granular access control to prevent unauthorized access from users of your enterprise IT data center.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 772, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '551fcf8dbe8fdc3140b9c79102fa083e', 'text': '• Ensure proper segmentation and isolation between the IT and OT/IIoT network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 772, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d0d49d894f0af5df215347c79646282', 'text': '• Secure API communication by ensuring encrypted communication between the orchestration and SDN layers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 772, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a70db60772ab0f17f78dd65632bbdcf6', 'text': '• Ensure enhanced visibility, monitoring, and anomaly detection on the management and control plane, including encrypted traffic of the IoT network slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 772, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ce1b571588f69326971879628f758167', 'text': '• Implement application security, including securing inter-NF communications and applying microsegmentation and application-level security controls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 773, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '30ed27f8c66ed2c27548cf61c29064ee', 'text': '• Create network security zones and anti-malware security controls within your data center and network infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 773, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '76e626944ca13229fd41abd08635742a', 'text': 'Priority of Security Controls to Secure Stage 1', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 773, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '99500af9a854016a7311fddbfbc5b518', 'text': 'Figure 11-17 illustrates the priority of security controls to secure Stage 1.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 773, 'parent\_id': '76e626944ca13229fd41abd08635742a', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '16341d9c21ad9939224130b0a7265277', 'text': 'Supply Chain Security - HW & SW OT & Infrastructure Granular User Security Access Controls Secure API security interoperability Application Level Anti-DDoS Security Vulnerability Access & Aggregation Management & Forensics Enhanced Visibility Slice Level Security Monitoring', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 773, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '17e1b352f92edcc8d3f31c7e18ce8858', 'text': 'Figure 11-17 Priority of Security Controls to Secure Stage 1', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 773, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c9319371c698822da03a88383297d1d4', 'text': 'The key threat security controls for securing Stage 1 are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 773, 'parent\_id': '17e1b352f92edcc8d3f31c7e18ce8858', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd48911f3c05a787e573fd85b481f4b21', 'text': '• Ensure you follow a robust process for supply chain security, including hardware and software of IIoT/IoT devices and IIoT network gateways.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 773, 'parent\_id': '17e1b352f92edcc8d3f31c7e18ce8858', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0a14de79a84cd357935691f878586a12', 'text': '• Ensure protection against DDoS and data exfiltration attacks from IoT devices controlled by C&C servers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 773, 'parent\_id': '17e1b352f92edcc8d3f31c7e18ce8858', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f9d5ee9b122c38c08d8e31934fe749dd', 'text': '• Implement granular access control to prevent unauthorized access from users of your enterprise IT data center.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 774, 'parent\_id': '17e1b352f92edcc8d3f31c7e18ce8858', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0592f6f83be6d742e39e81e8ce7b5570', 'text': '• Ensure proper segmentation and isolation between the IT and OT/IIoT network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 774, 'parent\_id': '17e1b352f92edcc8d3f31c7e18ce8858', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5ac4d4070132cb0fc039aaaf34164a6a', 'text': '• Secure API communication by ensuring encrypted communication between the orchestration and SDN layers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 774, 'parent\_id': '17e1b352f92edcc8d3f31c7e18ce8858', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'db1f295b34dd860f513a469a236410ad', 'text': '• Ensure enhanced visibility, monitoring, and anomaly detection on the management and control plane, including encrypted traffic of the IoT network slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 774, 'parent\_id': '17e1b352f92edcc8d3f31c7e18ce8858', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e7f07a6509e0102bf2c33a78ad67f4c7', 'text': '• Implement application security, including securing inter-NF communications and applying micro-segmentation and application-level security controls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 774, 'parent\_id': '17e1b352f92edcc8d3f31c7e18ce8858', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3d0946e52bb4ff0c401173aa9d26852c', 'text': '• Create network security zones and anti-malware security controls within your data center and network infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 774, 'parent\_id': '17e1b352f92edcc8d3f31c7e18ce8858', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '9d225afdec91c60c8c6124ab28c6ba5b', 'text': 'Priority of Security Controls to Secure Stage 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 774, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67f41e6f2310b2bc20aad844496cdebd', 'text': 'Figure 11-18 illustrates the priority of security controls to secure Stage 2.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 774, 'parent\_id': '9d225afdec91c60c8c6124ab28c6ba5b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '870a3e52e7b8dd0d20485c7b0d1159de', 'text': 'Supply Chain Security - HW & SW OT & Infrastructure Granular User Security ccess Controls Secure API security interoperability Anti-DDoS Application Level Security Access & Vulnerability Management & Aggregation Forensics Enhanced Visibility Slice Level Security Monitoring', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 775, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '4a834d2e2c3163b69b543ef1df8fc676', 'text': 'Figure 11-18 Priority of Security Controls to Secure Stage 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 775, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b69420750c94b78b76491a74abb1ba9e', 'text': 'The key threat security controls to secure Stage 2 are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 775, 'parent\_id': '4a834d2e2c3163b69b543ef1df8fc676', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e2f00ac90128a216c14893bb9fd42d7e', 'text': '• Ensure you follow a robust process for supply chain security, including hardware and software of IIoT/IoT devices and IIoT network gateways.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 775, 'parent\_id': '4a834d2e2c3163b69b543ef1df8fc676', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'adcb57b67833d7f6b7221aaaf7ea8b8f', 'text': '• Implement granular access control to prevent unauthorized user access from public service provider–integrated slices or NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 775, 'parent\_id': '4a834d2e2c3163b69b543ef1df8fc676', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '98214084120f44b1ede97d790cafe2f3', 'text': '• Secure interconnect between your smart manufacturing facility and public service providers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 775, 'parent\_id': '4a834d2e2c3163b69b543ef1df8fc676', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2fb6f7761119da32d8b9ef06cb1e4f66', 'text': '• Ensure secondary slice-level authentication if the integration with public networks requires implementation of slices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 775, 'parent\_id': '4a834d2e2c3163b69b543ef1df8fc676', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ca36614683a43d3821926c552dfedf8e', 'text': '• Implement protection against DDoS and data exfiltration attacks from IoT devices controlled by C&C servers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 775, 'parent\_id': '4a834d2e2c3163b69b543ef1df8fc676', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c2cdde8ad041900d57bffd17761aa621', 'text': '• Ensure proper segmentation and isolation between the IT and OT/IIoT network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 775, 'parent\_id': '4a834d2e2c3163b69b543ef1df8fc676', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c5460ef7336ac686b17c0643bc825f33', 'text': '• Secure API communication by ensuring encrypted communication between the orchestration and SDN layers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 776, 'parent\_id': '4a834d2e2c3163b69b543ef1df8fc676', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2707fba20165c0220cfc84602911d5ba', 'text': '• Ensure enhanced visibility, monitoring, and anomaly detection on the management and control plane, including encrypted traffic of the IoT network slice.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 776, 'parent\_id': '4a834d2e2c3163b69b543ef1df8fc676', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '039fa9336974b537b08dd4840e0803e8', 'text': '• Implement application security, including securing inter-NF communications and applying microsegmentation and application-level security controls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 776, 'parent\_id': '4a834d2e2c3163b69b543ef1df8fc676', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2ee084cbb63e48600dc52acb596c2552', 'text': '• Create network security zones and anti-malware security controls within your DC and network infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 776, 'parent\_id': '4a834d2e2c3163b69b543ef1df8fc676', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2f543520eb59ccfa65a56cf111096d77', 'text': 'Priority of Security Controls to Secure All Stages', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 776, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '56bb921b02451283d538869640038d9a', 'text': 'If you plan to deploy both stages together in the same cluster or different parts of the network, the following process will help you determine the key security controls required to ensure a secure rollout of both stages.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 776, 'parent\_id': '2f543520eb59ccfa65a56cf111096d77', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8746f8b614704d14b46fd9c7dd476928', 'text': 'Table 11-5 indicates the priority of the security controls for each of the stages and then helps you determine the priority of the security control when both stages of Scenario 2 are used in your NPN network. This table also helps you to understand the highest priority of each of the stages and then select that priority for the respective security control.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 776, 'parent\_id': '2f543520eb59ccfa65a56cf111096d77', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bb5b94ad1c07746b1ffb53d00407a50b', 'text': 'As an example, looking at the Slice-Level Security entry in Table 11-5, you see it categorized as a “low” security control for Stage 1 and as a “very high” security control for Stage 2. If you plan to deploy both stages, the highest security priority for the use case should be selected. In this case, slice-level security would be a “very high” security control.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 776, 'parent\_id': '2f543520eb59ccfa65a56cf111096d77', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '6faf2a5d5315508e22fe9c522ebd3a24', 'text': 'Stage 1 Stage 2 Both Stages Together Security Control Priority Priority Priority Supply Chain Security — Critical Critical Critical HW and SW Granular User Access Critical Critical Critical Controls Secure Interoperability Low Very High Very High Critical Critical Critical Application-Level Security Vulnerability Very High Very High Very High Management and Forensics Slice-Level Security Low Very High Very High Enhanced Visibility and Critical Critical Critical Monitoring Access and Aggregation High High High Anti-DDoS Very High Very High Very High API security Critical Critical Critical OT and Infrastructure Critical Critical Critical Security', 'metadata': {'text\_as\_html': '<table><thead><tr><th></th><th>Stage 1</th><th>Stage 2</th><th>Both Stages Together</th></tr></thead><tbody><tr><td>Security Control</td><td>Priority</td><td>Priority</td><td>Priority</td></tr><tr><td>Supply Chain Security — HW and SW</td><td>Critical</td><td>Critical</td><td>Critical</td></tr><tr><td>Granular User Access Controls</td><td>Critical</td><td>Critical</td><td>Critical</td></tr><tr><td>Secure Interoperability</td><td>Low</td><td>Very High</td><td>Very High</td></tr><tr><td>Application-Level Security</td><td>Critical</td><td>Critical</td><td>Critical</td></tr><tr><td>Vulnerability Management and Forensics</td><td>Very High</td><td>Very High</td><td>Very High</td></tr><tr><td>Slice-Level Security</td><td>Low</td><td>Very High</td><td>Very High</td></tr><tr><td>Enhanced Visibility and Monitoring</td><td>Critical</td><td>Critical</td><td>Critical</td></tr><tr><td>Access and Aggregation</td><td>High</td><td>High</td><td>High</td></tr><tr><td>Anti-DDoS</td><td>Very High</td><td>Very High</td><td>Very High</td></tr><tr><td>API security</td><td>Critical</td><td>Critical</td><td>Critical</td></tr><tr><td>OT and Infrastructure Security</td><td>Critical</td><td>Critical</td><td>Critical</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 777, 'parent\_id': '2f543520eb59ccfa65a56cf111096d77', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '24aa033714a66d2c7d9644a6edbfadf1', 'text': 'Table 11-5 Summary of Priority Security Controls for Scenario 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 777, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd389cc37f4142d435b7c29c57e09d02b', 'text': 'Figure 11-19 illustrates the priority of security controls to secure the network when both Stage 1 and Stage 2 are used in your 5G NPN deployment.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 777, 'parent\_id': '24aa033714a66d2c7d9644a6edbfadf1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'f6bcd6613625137bd5879bf4411e0110', 'text': 'Supply Chain Security - HW & SwW OT & Infrastructure Granular User Security Access Controls Secure API security interoperability Anti-DDoS Application Level Security Vulnerability Access & Aggregation Management & Forensics Enhanced Visibilit & Monitoring Slice Level Security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 778, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '8951501edbd492702767894a4490c91c', 'text': 'Figure 11-19 Priority of Security Controls to Secure Both Stages in Scenario 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 778, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8abfa78589e92f9ba71520b899caed8f', 'text': 'The key threat security controls for securing Stages 1 and 2 are as follows:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 778, 'parent\_id': '8951501edbd492702767894a4490c91c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '22fa8dcc41d86957171c651312ba6aca', 'text': '• Ensure you follow a robust process for supply chain security, including hardware and software of IIoT/IoT devices and IIoT network gateways.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 778, 'parent\_id': '8951501edbd492702767894a4490c91c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ec6700c5fe69148285df2c30d6e6d615', 'text': '• Implement granular access control to prevent unauthorized user access from public service provider–integrated slices or NFs.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 778, 'parent\_id': '8951501edbd492702767894a4490c91c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a676f2323c6762a4994f95502d55677d', 'text': '• Ensure protection against DDoS and data exfiltration attacks from IoT/IIoT devices controlled by C&C servers.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 778, 'parent\_id': '8951501edbd492702767894a4490c91c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c158f723334144a8b393615123caf4f9', 'text': '• Implement proper segmentation and isolation between the IT and OT/IIoT network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 778, 'parent\_id': '8951501edbd492702767894a4490c91c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a1869ae012f32d83027fd311c6eb339b', 'text': '• Implement API security catering for the Top 10 OWASP threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 778, 'parent\_id': '8951501edbd492702767894a4490c91c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '27d6231cee62f34ae835d5d20ff99975', 'text': '• Implement enhanced visibility, monitoring, and anomaly detection on the management and control plane, including encrypted API traffic.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 778, 'parent\_id': '8951501edbd492702767894a4490c91c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '98ab295da218889c7b3b15e12b1b136a', 'text': '• Implement application security, including securing inter-NF communications and applying microsegmentation and application-level security controls.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 779, 'parent\_id': '8951501edbd492702767894a4490c91c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ffa39c9aa9d40ea9a4c1f121485d01c8', 'text': '• Create network security zones and anti-malware security controls within your data center and network infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 779, 'parent\_id': '8951501edbd492702767894a4490c91c', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '693e86125b36d1797759e71c0ce2cc9d', 'text': 'Summary of Priority Security Controls for Scenario', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 779, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '65279cc926c0419b3e3977f100a6a113', 'text': 'Summary of Priority Security Controls for Scenario 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 779, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'edf2822c42bf28a477b2a698b46ee8b7', 'text': 'Table 11-6 illustrates the priority of security controls to secure Scenario 2.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 779, 'parent\_id': '65279cc926c0419b3e3977f100a6a113', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': 'caa1d9a258f60aa2f2426d984ef908f5', 'text': 'Security Priority of Mapping Notes Control Investment Investment Priority to Deployment Stages Critical Supply Chain Required from Mandatory to be verified and Security [nd] initial staging, validated during initial HW and SW onboarding and deployment and throughout implementation of the operation of live Stage 1 networks. Granular User Critical Required from Mandatory during the initial Access Controls initial staging, deployment and throughout onboarding and the operation of live networks implementation of to mitigate unauthorized Stage 1 to secure access from the IT network. access during staging of equipment and CNFs Secure Stage 1: Low Required in Stage Mandatory once you move 2 Interoperability Stage 2: away from standalone NPN Very High deployment and integrate with CSP, data network, and public cloud. Application- Critical Required from Mandatory to be included in Level Security initial staging, Stage 1, including CI/CD onboarding and processes by your implementation of development team. Stage 1 to ensure secure staging of equipment and CNFs', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Security Control</th><th>Priority of Investment</th><th>Mapping Investment Priority to Deployment Stages</th><th>Notes</th></tr></thead><tbody><tr><td>Supply Chain Security [nd] HW and SW</td><td>Critical</td><td>Required from initial staging, onboarding and implementation of Stage 1</td><td>Mandatory to be verified and validated during initial deployment and throughout the operation of live networks.</td></tr><tr><td>Granular User Access Controls</td><td>Critical</td><td>Required from initial staging, onboarding and implementation of Stage 1 to secure access during staging of equipment and CNFs</td><td>Mandatory during the initial deployment and throughout the operation of live networks to mitigate unauthorized access from the IT network.</td></tr><tr><td>Secure Interoperability</td><td>Stage 1: Low Stage 2: Very High</td><td>Required in Stage 2</td><td>Mandatory once you move away from standalone NPN deployment and integrate with CSP, data network, and public cloud.</td></tr><tr><td>Application- Level Security</td><td>Critical</td><td>Required from initial staging, onboarding and implementation of Stage 1 to ensure secure staging of equipment and CNFs</td><td>Mandatory to be included in Stage 1, including CI/CD processes by your development team.</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 780, 'parent\_id': '65279cc926c0419b3e3977f100a6a113', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '819aa4ee1de50dccbf66439bb188c10f', 'text': "Vulnerability Very High Required from Mandatory to be included in Management and Stage 1 but less Stage 1 to detect and mitigate Forensics priority than any identified vulnerabilities. Access control, Supply Chain, Monitoring and API security. Slice-Level Very High Required before Mandatory to be deployed Security Network Slicing is during Stage 2 when being implemented integrated with CSP. Enhanced Critical Required from Mandatory during initial Visibility and initial staging, deployment and throughout Monitoring onboarding and the operation of live networks. implementation of Stage 1 Access and Very High Required if public Mandatory if you are using a (network network is used in Aggregation public network for back- dependent) backhaul/xHaul hauling. If you are using your and if country own back-haul transport regulators have network, you can implement advised using it as these security controls when a mandatory you have integration points security control. with third-party back-haul transport providers. Some countries have a mandatory requirement of using a security gateway in the back haul/xHaul defined by the country's regulator. Anti-DDoS Very High Required mainly Mandatory to mitigate DDoS after network goes attacks from loT and IloT live or closer to devices connected to CSP, being live public cloud, or data networks. API Security Critical Required from Mandatory during initial initial staging, deployment and throughout onboarding and the operation of live implementation of networks. Stage 1 OT and Critical Required from Mandatory during initial Infrastructure initial staging, deployment and throughout Security onboarding and the operation of live implementation of networks. Stage 1", 'metadata': {'text\_as\_html': "<table><thead><tr><th>Vulnerability Management and Forensics</th><th>Very High</th><th>Required from Stage 1 but less priority than Access control, Supply Chain, Monitoring and API security.</th><th>Mandatory to be included in Stage 1 to detect and mitigate any identified vulnerabilities.</th></tr></thead><tbody><tr><td>Slice-Level Security</td><td>Very High</td><td>Required before Network Slicing is implemented</td><td>Mandatory to be deployed during Stage 2 when being integrated with CSP.</td></tr><tr><td>Enhanced Visibility and Monitoring</td><td>Critical</td><td>Required from initial staging, onboarding and implementation of Stage 1</td><td>Mandatory during initial deployment and throughout the operation of live networks.</td></tr><tr><td>Access and Aggregation</td><td>Very High (network dependent)</td><td>Required if public network is used in backhaul/xHaul and if country regulators have advised using it as a mandatory security control.</td><td>Mandatory if you are using a public network for back- hauling. If you are using your own back-haul transport network, you can implement these security controls when you have integration points with third-party back-haul transport providers. Some countries have a mandatory requirement of using a security gateway in the back haul/xHaul defined by the country's regulator.</td></tr><tr><td>Anti-DDoS</td><td>Very High</td><td>Required mainly after network goes live or closer to being live</td><td>Mandatory to mitigate DDoS attacks from loT and IloT devices connected to CSP, public cloud, or data networks.</td></tr><tr><td>API Security</td><td>Critical</td><td>Required from initial staging, onboarding and implementation of Stage 1</td><td>Mandatory during initial deployment and throughout the operation of live networks.</td></tr><tr><td>OT and Infrastructure Security</td><td>Critical</td><td>Required from initial staging, onboarding and implementation of Stage 1</td><td>Mandatory during initial deployment and throughout the operation of live networks.</td></tr></tbody></table>", 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 781, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Header', 'element\_id': 'a87b5f334408a7b1f489cc1c85135db8', 'text': 'Table 11-6 Investment Priority for Scenario 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 782, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5a32cb0af8184e38da29b4e035a00f02', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 782, 'parent\_id': 'a87b5f334408a7b1f489cc1c85135db8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ec6de57bef82b82d6a503139930fb657', 'text': 'As seen from the aforementioned scenarios, you can prioritize your investments based on the phases of 5G network deployment, the use cases planned to be deployed, and the preferred architecture. As compared to legacy technologies, 5G brings in the requirement to secure network functions at the application level, including user-to-application mapping, application dependency mapping, application-level vulnerability management, and securing the API communications. You should have the following critical security controls at a bare minimum, even before you start any deployment of 5G 3GPP and non-3GPP equipment and NFs. In other words, if you would like to prioritize your investment in securing 5G deployments, the following list should be at the top of your priority list for security:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 782, 'parent\_id': '5a32cb0af8184e38da29b4e035a00f02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2bd1d2f9315aa8c19c643f464aa1f3af', 'text': '• Controls related to supply chain security, such as image authentication and vulnerability detection', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 782, 'parent\_id': '5a32cb0af8184e38da29b4e035a00f02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd4699ed430ab4b2c91bd5a303434f53d', 'text': '• Granular access control (users and devices)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 782, 'parent\_id': '5a32cb0af8184e38da29b4e035a00f02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8ee419f4691c9797cdef5fc43791e89e', 'text': '• End-to-End visibility and monitoring, including anomaly detection and detection of malware in the encrypted layer (specifically for external API communications)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 782, 'parent\_id': '5a32cb0af8184e38da29b4e035a00f02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd39f68007e10a66f497d6c57ca5529a5', 'text': '• Application-level security, including application-level policy enforcement, threat detection, and response', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 782, 'parent\_id': '5a32cb0af8184e38da29b4e035a00f02', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'f34d84586cb3511159f4ad0760dbb095', 'text': 'Acronyms Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 782, 'parent\_id': 'a87b5f334408a7b1f489cc1c85135db8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9ccdf929fa64479cc9af3cdb07ed7164', 'text': 'The following table expands the key acronyms used in this chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 782, 'parent\_id': 'f34d84586cb3511159f4ad0760dbb095', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '06759b3f96eb59bf47874c46cc435244', 'text': 'Acronym Expansion 3GPP Third-Generation Partnership Project 5GC 5G Core API Application programming interface AUSF Authentication Server Function C&C Control and command center CD Continuous development CI Continuous integration CNF Cloud-Native Function CSC Communication service consumer CSp Communication service provider DDoS Distributed denial of service', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Acronym</th><th>Expansion</th></tr></thead><tbody><tr><td>3GPP</td><td>Third-Generation Partnership Project</td></tr><tr><td>5GC</td><td>5G Core</td></tr><tr><td>API</td><td>Application programming interface</td></tr><tr><td>AUSF</td><td>Authentication Server Function</td></tr><tr><td>C&amp;C</td><td>Control and command center</td></tr><tr><td>CD</td><td>Continuous development</td></tr><tr><td>CI</td><td>Continuous integration</td></tr><tr><td>CNF</td><td>Cloud-Native Function</td></tr><tr><td>CSC</td><td>Communication service consumer</td></tr><tr><td>CSp</td><td>Communication service provider</td></tr><tr><td>DDoS</td><td>Distributed denial of service</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 783, 'parent\_id': 'f34d84586cb3511159f4ad0760dbb095', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '3ecc591975329486d1bb7d15585e8a41', 'text': 'DoS Denial of service eMBB Enhanced mobile broadband HW Hardware loT Internet of Things M2M Machine-to-machine MBB Mobile broadband MEC Multi-access edge compute MitM Man in the middle NF Network Function NPN Non-public network NSaaS Network slice as a service NW Network oT Operational technology O-RAN Open RAN PNI- NPN Public network integrated non-public network RASP Runtime Application Self-Protection RAN Radio access network RAT Radio access technology SSL Secure Sockets Layer TLS Transport Layer Security UDM Unified data management UE User equipment UPF User Plane Function VNF Virtual Network Function VRAN Virtual RAN WAF Web application firewall', 'metadata': {'text\_as\_html': '<table><thead><tr><th>DoS</th><th>Denial of service</th></tr></thead><tbody><tr><td>eMBB</td><td>Enhanced mobile broadband</td></tr><tr><td>HW</td><td>Hardware</td></tr><tr><td>loT</td><td>Internet of Things</td></tr><tr><td>M2M</td><td>Machine-to-machine</td></tr><tr><td>MBB</td><td>Mobile broadband</td></tr><tr><td>MEC</td><td>Multi-access edge compute</td></tr><tr><td>MitM</td><td>Man in the middle</td></tr><tr><td>NF</td><td>Network Function</td></tr><tr><td>NPN</td><td>Non-public network</td></tr><tr><td>NSaaS</td><td>Network slice as a service</td></tr><tr><td>NW</td><td>Network</td></tr><tr><td>oT</td><td>Operational technology</td></tr><tr><td>O-RAN</td><td>Open RAN</td></tr><tr><td>PNI- NPN</td><td>Public network integrated non-public network</td></tr><tr><td>RASP</td><td>Runtime Application Self-Protection</td></tr><tr><td>RAN</td><td>Radio access network</td></tr><tr><td>RAT</td><td>Radio access technology</td></tr><tr><td>SSL</td><td>Secure Sockets Layer</td></tr><tr><td>TLS</td><td>Transport Layer Security</td></tr><tr><td>UDM</td><td>Unified data management</td></tr><tr><td>UE</td><td>User equipment</td></tr><tr><td>UPF</td><td>User Plane Function</td></tr><tr><td>VNF</td><td>Virtual Network Function</td></tr><tr><td>VRAN</td><td>Virtual RAN</td></tr><tr><td>WAF</td><td>Web application firewall</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 784, 'parent\_id': 'f34d84586cb3511159f4ad0760dbb095', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ece8f717f97b99613a9701d2c2863fa1', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 785, 'parent\_id': 'a87b5f334408a7b1f489cc1c85135db8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '67e53824bfb616045f9cbfc35bc3538b', 'text': 'Pramod Nair, “Securing Your 5G Infrastructure to the Edge and Beyond Cisco Public,” April 1, 2021', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 785, 'parent\_id': 'ece8f717f97b99613a9701d2c2863fa1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'dd34cd00fe3388b90934ca7f3cc22332', 'text': 'Pramod Nair, “Securing 5G and Evolving Architectures,” Cisco Knowledge Networks, Cisco Public, September 17, 2020', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 785, 'parent\_id': 'ece8f717f97b99613a9701d2c2863fa1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b239a402146e3ddcc746740cb08418e0', 'text': 'Jason Longley and Pramod Nair, “Securing the 5G Core (5GC) and Evolved Packet Core (EPC) with Cisco Security,”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 785, 'parent\_id': 'ece8f717f97b99613a9701d2c2863fa1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '57901cc08fe1cdf3fa7c21902fdad5a0', 'text': 'https://www.cisco.com/c/en/us/solutions/collateral/service- provider/service-provider-security-solutions/white-paper-c11- 742166.pdf', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 785, 'parent\_id': 'ece8f717f97b99613a9701d2c2863fa1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '5ae59d3c767a7b1f14fe9068723aa800', 'text': '3GPP TS 33.501. V17.1.0, “Security architecture and procedures for 5G System.”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 785, 'parent\_id': 'ece8f717f97b99613a9701d2c2863fa1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4e4b720e8fa013a5807f0dff26ec36d8', 'text': 'https://www.cisco.com/c/dam/en\_us/solutions/iot/demystifying-5g- industrial-iot.pdf', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 785, 'parent\_id': 'ece8f717f97b99613a9701d2c2863fa1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd12b9e09294273060e9b691c8a17aa47', 'text': 'https://www.portshift.io/', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 785, 'parent\_id': 'ece8f717f97b99613a9701d2c2863fa1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '92b9ff7fd8433730dac26b5537b10542', 'text': 'https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Solution\_ Briefs/IA\_Networking\_Solution\_Brief.html', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 785, 'parent\_id': 'ece8f717f97b99613a9701d2c2863fa1', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'c51ee8df9f5e83be1af7ba51bdbec445', 'text': 'Part IV: Emerging Discussions', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 786, 'parent\_id': 'a87b5f334408a7b1f489cc1c85135db8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'text': 'Chapter 12. 5G and Beyond', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 787, 'parent\_id': 'a87b5f334408a7b1f489cc1c85135db8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '625112281186dfdd84ae83d70df4d3a5', 'text': 'After reading this chapter, you should have a better understanding of the following topics:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 787, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'caeb967efc28bdb85da871d2d8918b9d', 'text': '• Adoption of 5G standalone technology', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 787, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '45df3e896ba462d1624ab2ff76fe292b', 'text': '• Adaptation of 5G standalone technology on fulfilling new use cases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 787, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b8a946bd8809762af9fcc74b78da2363', 'text': '• Convergence of non-3GPP and 3GPP technologies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 787, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '09d1e93071295fae2558b2a77599799d', 'text': '• Application of AI and ML in securing 5G and evolving technologies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 787, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9aa8534e270a27b11e9c0293b78a4951', 'text': '• Importance of deploying crypto-agile mobile networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 787, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '029c0758760805a115de989b29e51e41', 'text': "The content in this chapter will continue to evolve, and I want to keep you up to date on developments. I will update the chapter occasionally with relevant new content and insights on the book's website at www.informit.com. To access the chapter, start by establishing a login at www.informit.com and register your book. To do so, simply go to www.informit.com/register and enter the ISBN of the print book: 9780137457939. Answer the challenge question as proof of purchase. Click the “Access Bonus Content” link in the “Registered Products” section of your account page to be taken to the page where your downloadable content is available.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 787, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c6f1edce9d80cb9fb2ed0cf04ddc6997', 'text': 'This chapter takes you through the key areas for pragmatic adoption of 5G and evolving technologies, the architecture evolution to cater for 3GPP and non- 3GPP convergence, the use of artificial intelligence (AI) and machine learning (ML) to enhance security posture, and the methods to ensure the crypto-agility of your network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 787, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7909a8637e3441a834ba91d109860e8a', 'text': 'This chapter would be of particular interest to the following individuals and teams from enterprise/5G service providers deploying 5GC and cybersecurity vendors planning product developments for 5G security use cases:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 787, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8e8b3c7693f0c73bd5d943c63e2b5de5', 'text': '• Security leaders within government organizations who need to prioritize investments in security', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 787, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1db1bbcef349de6f84e77051b4e916a7', 'text': '• Management consultants advising governments and service providers on 5G security investment', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 787, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6307920aaae9d968337727fa1ab789ba', 'text': '• CSO and CTO teams from service providers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 787, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3a15ce1711b84a6d284b90f2fb88deda', 'text': '• CSO and CTO teams from enterprise teams deploying non-public networks (NPN)/private 5G', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 788, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f2320427a33dc53bd905acf735a0631', 'text': '• Cybersecurity vendor security architects looking to secure 5GC deployments for their customers', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 788, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '19b9af0ba29363dd017cd621c42ce12e', 'text': '• Cybersecurity vendor product managers looking for use cases or features to enhance security products to cater for secure 5G deployments', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 788, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '47d53efd4b9b8892e18cad6288064cbf', 'text': '5G Standalone (SA) is the first cellular technology that brings in true openness to 3GPP network deployments. There is industry-wide anticipation in the range of pragmatic use cases that can be enabled through 5G. But if we look at the history of telecommunications, the lifespan the 2G, 3G, 4G technologies is each around 10 years.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 788, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ce28820ba87cbd6afff4722c80825e3e', 'text': 'Various service providers have announced that 2G technology will be switched off to free the spectrum to deploy newer technologies. Many have already switched off 2G and have performed spectrum re-farming. Although 2G has been superseded by technologies such as 3G and 4G, it is still widely used across Europe, Asia, Africa, and Central and South America, specifically in rural areas and highways. Switching off 2G in many countries will leave the population in rural areas vulnerable and without any coverage. There are also many point-of-sale (PoS) terminals that still use 2G due to low-cost chipsets, leading to lower prices for the terminals. Therefore, the decision to terminate an old technology and adopt a new one is not just based on “getting on the new technology bandwagon” but is primarily use case and customer profile driven.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 788, 'parent\_id': '487f1b4e0faa6f5fa709fb37bf2da3c0', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '19943140a1236cfeb9205e7c7a059bce', 'text': 'Adoption and Adaptability of 5G and Evolving Technologies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 788, 'parent\_id': 'a87b5f334408a7b1f489cc1c85135db8', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1e3144ce9d95115fc7f7e9cca2e7bd85', 'text': 'The timeline of 5G SA adoption will depend on the timeline for deploying your use cases and the availability of 5G-capable handsets. Fully fledged 5G inter- public land mobile network (PLMN) interconnect might take at least 2–3 years, as you will need your roaming partners to be fully 5G compatible as well. The initial 5G specifications came through 3GPP release 15 (rel-15), which was primarily based on 5G NSA. Rel-16 then brought in 5G SA–related features, which are now being widened to enhance the network slice as a service (NSaaS), voice-to-everything (V2X), integrations with non-3GPP networks, and so on. Figure 12-1 illustrates the timeline of Rel-17 and work package approval for Rel-18.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 788, 'parent\_id': '19943140a1236cfeb9205e7c7a059bce', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'faee22efd66d83dc64b891a65ebcd9f1', 'text': 'Rel7 Protocol Rel-17 Stage Rel-17 Stage 2 Freeze 3 Freeze Coding Freeze Rel-18 Package Approval From: www.3GPP.org/specifications/67-releases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 789, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '33dd9310bdc4974ac868dc789d26d0c8', 'text': 'From: www.3GPP.org/specifications/67-releases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 789, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7318c5945ed74bbfcbfdc7033fe0dd86', 'text': 'Figure 12-1 Timeline of Rel-17 and Work Package Approval for Rel-18', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 789, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '1657ebe4f0f0c17b7983c88c147d59ad', 'text': "At the same time, certain industry verticals such as critical infrastructures as well as military and defense organizations are looking to deploy 5G NPNs to make use of the advantages provided by 5G. Depending on the chosen deployment model, such organizations will require integration with the service provider's 5G Core (5GC) Network Function (NF). You might also see an", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 789, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c7112ab82dbeb4f9405a84e04211c734', 'text': 'abundance of 5G-capable phones in the near future, which is a very important ecosystem to consider before you plan to launch 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 790, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '994286d2e725ad078337a5222aff041f', 'text': 'To provide service to existing subscribers and to enable new 5G use cases, you will require legacy technologies as well as the adoption of 5G technology. Therefore, although investing in 5G security controls is important, you also need to ensure that the security controls for legacy technologies are not ignored. Figure 12-2 illustrates some of the key use cases pinpointed by 5G and evolving technologies.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 790, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '238a7367b9c3a7fd10e3578e93d65a6e', 'text': '5G and Beyond', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 790, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a721c439ccd2d463a51abd66d90147a5', 'text': '5G and Beyond Smart Home Smart Factory Fixed Wireless Broadband Smart City Industrial Automation 3GPP and Non-3GPP Convergence Enhanced indoor and outdoor coverage Autonomous vehicle VX Telghealth Asset Tracking Remote Monitoring Smart City', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 790, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'bd0f1cf9247e7e0bb5d6cf45803f669b', 'text': 'Figure 12-2 Use Cases Focused on Technologies 5G and Beyond', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 790, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '893ef0d67664fdfda807db408bf62cd9', 'text': 'The range of uses cases targeted for 5G and evolving technologies is much broader than legacy technologies. 5G and evolving networks will transform how you live, work, and travel. To enable this transformation, the standards bodies are working behind the scenes to provide you with a seamless', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 790, 'parent\_id': 'bd0f1cf9247e7e0bb5d6cf45803f669b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '42d7d55290c76cbff370fee130b14b15', 'text': 'experience. This tight interworking among standards development organizations (SDOs) has never been so important. For example, several SDOs are working together on machine-to-machine standards activity. These SDOs include the Association of Radio Industries and Businesses (ARIB) and the Telecommunication Technology Committee (TTC) of Japan; the Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association (TIA) of the United States; the China Communications Standards Association (CCSA); the European Telecommunications Standards Institute (ETSI); and the Telecommunications Technology Association (TTA) of Korea.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 791, 'parent\_id': 'bd0f1cf9247e7e0bb5d6cf45803f669b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '48de4defb7dcf0ea20d51728aff1a606', 'text': 'Once you have deployed 5G SA, you will see a range of use cases that require flexible 5G deployment models. Some deployment models require your infrastructure, such as multi-access edge compute (MEC), to be shared with certain industry verticals, and in some cases you will need to peel off a part of your network and offer it to industry verticals using an NSaaS offering. Such models will expose your network to new risks related to untrusted private and public network integrations. Fulfilling certain use cases might require you to onboard untrusted workloads, leading to risks such as compromised onboarded workloads exposing your entire network to attackers. While it is possible to detect and mitigate such risks manually at a small scale, it is an extremely difficult and nearly impossible task to do manually at a large scale. This requires you to think about scale and feature parity across virtual deployments —be it virtual machines, containers on virtual machines and bare metal, or serverless deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 791, 'parent\_id': 'bd0f1cf9247e7e0bb5d6cf45803f669b', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'ed61703d787cb1a9cc715d5e47f5a213', 'text': 'Convergence of Wi-Fi and Evolving Cellular Technologies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 791, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '44ea4461befc3f1b1c3ccc9fb7d82b0c', 'text': "ITU-R is an international decision-making body that is in charge of radio communication regulations with 193 member states. It also manages global mobile telecommunication standards and has provided guidance and a roadmap for next-generation communication R&D by defining the vision for next- generation mobile telecommunication, such as 4G and 5G. Starting with completing the 6G Vision by 2023, ITU-R plans to develop technical requirements and recommendations for 6G through industry standards organizations such as 3GPP. Out of those candidate technologies for 6G, the technologies that pass ITU-R's evaluation will be approved as the global standards for 6G around 2030.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 791, 'parent\_id': 'ed61703d787cb1a9cc715d5e47f5a213', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'be9c7a8e3594b7c9bbf58c15d019d298', 'text': 'ITU-R Working Party 5D (WP 5D) has started to develop a draft new recommendation on IMT Vision for 2030 and beyond, which will include 6G. The 6G Vision Group was newly launched at the ITU-R meeting in 2021. This group is in charge of establishing the 6G Vision, which includes defining the key capabilities, working on technology development, and creating timelines on standardization and commercialization of 6G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 792, 'parent\_id': 'ed61703d787cb1a9cc715d5e47f5a213', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c7b0b3766915bb8935655a70586d3415', 'text': 'IMT Vision for 2030 and beyond aims at a hybrid dense network consisting of multiple networks (3GPP and non-3GPP), with the desired end result of upgrading existing technologies instead of replacing the technology being used.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 792, 'parent\_id': 'ed61703d787cb1a9cc715d5e47f5a213', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b86dce145197e89bc08d4caa65bcb8b4', 'text': "Non-3GPP networks like Wi-Fi 6 and 3GPP networks like 5G are built from the same foundation of providing better capacity and throughput, supporting new use cases and applications, and enabling massive IoT. Although it's not the first time the topic of Wi-Fi versus cellular technologies has come up, now the discussions are about Wi-Fi and cellular technologies instead of Wi-Fi versus cellular technologies. Going forward, any upcoming standard and specification will focus on bringing 3GPP and non-3GPP networks closer.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 792, 'parent\_id': 'ed61703d787cb1a9cc715d5e47f5a213', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '37129bfba03a8e0e1ccd0a496422e2b0', 'text': 'IEEE 802.11be Extremely High Throughput (EHT), likely to be designated as Wi-Fi 7, is the potential next amendment of the Wi-Fi 802.11 standard, which is currently at 802.11ax (also called Wi-Fi 6). IEEE 802.11be will be built on 802.11ax, focusing on indoor and outdoor operation with stationary and pedestrian speeds in the 2.4, 5, and 6 GHz frequency bands. IEEE 802.11be (Wi-Fi 7) standardization is expected to be ready by 2024. This is around the time when networks will be deploying Rel-17 and initial Rel-18 3GPP 5G networks. The technology evolution in 3GPP cellular networks and Wi-Fi will lead to increased coexistence between them, and service providers might opt for a converged packet core for offering bundled services with Wi-Fi and 5G.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 792, 'parent\_id': 'ed61703d787cb1a9cc715d5e47f5a213', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '17e4ea4350b1cfdb2849550d3968263c', 'text': 'Looking at the overall cost of managing Wi-Fi for large enterprises, network slice as a service (NSaaS) might be an alternative that some might opt for going forward. There was always an option of enterprises choosing 4G instead of Wi-Fi, but the architecture was too constrained, and there was a need for using proprietary solutions to enable a seamless user experience. Looking at the ongoing Rel-17 work items and expected Rel-18 work items, there is a lot of work planned for non-3GPP and 3GPP integrations both at the user device domain and the packet core domain. This might be attractive for large enterprises that might prefer using network slices from service providers, leading to a seamless user experience with improved cost optimization.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 792, 'parent\_id': 'ed61703d787cb1a9cc715d5e47f5a213', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '056e22ea5f4cb3a13aad337b62023006', 'text': 'Specifically for use cases such as smart cities, the convergence of Wi-Fi and 5G will see increased adoption because many of the free wireless options will still be provided by Wi-Fi (Wi-Fi 7), and critical infrastructure components will use 5G due to enhanced security, support of ultra-reliable low latency communications (URLLC) for vehicle-to-everything (V2X), and customized use case offerings from service providers or non-public network (NPN) deployment by the industry verticals catering for smart city use cases. New 5G features, such as integration of 5GC Core with untrusted and trusted non-3GPP networks, bring the non-3GPP and 3GPP technologies closer.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 793, 'parent\_id': 'ed61703d787cb1a9cc715d5e47f5a213', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3ce0b4024070828fe94c83fac1fd9360', 'text': '3GPP has already started work in having closer integration between 3GPP and non-3GPP networks, starting with Rel-16. Figure 12-3 illustrates a non- roaming architecture for 5GC with untrusted non-3GPP access.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 793, 'parent\_id': 'ed61703d787cb1a9cc715d5e47f5a213', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '3c92577c99ea0f275656620dfceeb7d8', 'text': '( ) N2 AMF N1 SMF 3GPP Access N3 N4 N2 Data N3IWF N3 UPF Network N1 HPLMN NWu B A T PR, T PErTr P T T L L L L LT N1 Y2 Non-3GPP |\\ = Network ® -y — ,,’?\\ Untrusted Non- JGPP Access', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 793, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '33d94f910e5707987ddb55b486458edb', 'text': 'Untrusted Non- JGPP Access', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 793, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6c571f9a27a56ba31c3ef89f604fe3b4', 'text': 'Figure 12-3 Non-Roaming Architecture for 5GC with Untrusted Non- 3GPP Access', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 794, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '440fbde3f3a5842e14a0874cabaa5123', 'text': 'As shown in Figure 12-3, the Non-3GPP Interworking Function (N3IWF) performs routing of messages for the non-3GPP network. N3IWF connects to the User Plane Function (UPF) using the N3 interface and connects the control plane to the Access and Mobility Management Function (AMF) using the N2 interface.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 794, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c056a23120fc84dbb5108e24e124757e', 'text': 'Figure 12-4 illustrates non-roaming architecture for 5GC with trusted non- 3GPP access.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 794, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'd5c55ba10a800328082dba549400ae5b', 'text': '( ) /\_Au Nt ] SHF N1 3GPP N3 Access N4 N2 Data UPF Network HPLMN N3 Trusted N — Non-3GPP pra— (] Ta Gateway Wt Function i Tn TNAP ™F | Trusted Non-3GPP Access Network (TNAN)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 794, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '2e8e942a4ddcaa7d1497a9faefb11b99', 'text': 'Trusted Non-3GPP Access Network (TNAN)', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 794, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3336c4f8d861f6b87dfba9c7d21d2751', 'text': 'Figure 12-4 Non-Roaming Architecture for 5GC with Trusted Non-3GPP Access', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 794, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'aa6eafe8d3875dadabcf060a61ca2481', 'text': 'Access', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 794, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f01765ba95ceef700f7f8ecdeb795818', 'text': 'The key components of the non-roaming architecture for 5GC with trusted non-3GPP access, as illustrated in the Figure 12-4, are discussed next.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 795, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'c19f1441322f5c0ab3cfc70fe4244185', 'text': 'The Trusted Non-3GPP Access Network (TNAN) supports WLAN access technology such as Wi-Fi and consists of a Trusted Non-3GPP Access Point (TNAP) and a Trusted Non-3GPP Gateway Function (TNGF). The TNGF integrates with the 5G Core network control plane and user plane functions via the N2 and N3 interfaces, respectively.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 795, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '89b8598f5a1ee50ae2fd801f250242f4', 'text': '3GPP specifications also discuss the integration to allow non-5G-capable devices to access 5GC. The devices that do not support 5GC NAS signaling over WLAN access are referred to as non-5G-capable over WLAN (N5CW) devices. N5CW devices are not capable of operating as 5G UE that supports 5GC NAS signaling over a WLAN access network; however, they are capable of operating as 5G UE over NG-RAN, as shown in Figure 12-5.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 795, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7a63bd99cb194105984273d959abb28d', 'text': 'Figure 12-5 illustrates non-roaming and LBO roaming architecture for supporting 5GC access from N5CW devices.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 795, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': '4904ce8970fbdd81c90ee1323cc9bf21', 'text': 'N1t AMF SMF \\ N2 Data UPF Network N3 Trusted Trusted N — WLAN WLAN —M Access Yw Interworkin Point Non-5G-Capable over WLAN g Function (NSCW) device TWAP TWIF Trusted WLAN Access Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 795, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'cc756e118e5dc49a6a15dd38a7767467', 'text': 'Trusted WLAN Access Network', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 795, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '630f1159e7cfc9615bd9a9a3af9c8036', 'text': 'Figure 12-5 Non-Roaming and LBO Roaming Architecture for Supporting 5GC Access from N5CW Devices', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 796, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '79f4d3858fe5503c13ba0799ef978452', 'text': 'The key components of the architecture for supporting 5GC access from non- 5G-capable devices, as illustrated in the Figure 12-5, are discussed next.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 796, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ddcc30e597a74e33118c2b1ecfdf1574', 'text': "A trusted WLAN access network is a particular type of Trusted Non-3GPP Access Network (TNAN) that supports a WLAN access technology such as Wi-Fi. It's composed of a Trusted WLAN Access Point (TWAP) and a Trusted WLAN Interworking Function (TWIF). TWAP is a type of Trusted Non-3GPP Access Point (TNAP) that supports a WLAN access technology such as Wi-Fi. To support 5GC access from N5CW devices, a trusted WLAN access network must support the Trusted WLAN Interworking Function (TWIF). TWIF provides interworking functionality that enables N5CW devices to access 5GC. When an N5CW device performs an EAP-based access authentication procedure to connect to a trusted WLAN access network, the N5CW device may simultaneously be registered to a 5GC of a PLMN. The 5GC registration is performed by the TWIF function in the trusted WLAN access network, on behalf of the N5CW device.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 796, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ba0e8e886044ccc8311018bc80975281', 'text': 'These integrations, with enhanced security being worked on by 3GPP, will enable closer integration of 3GPP and non-3GPP technologies and also allow non-5G-capable devices to access 5GC. However, practical deployments for these architectures are not estimated to be widely available until 2023 or 2024, as there is further work to be done by both UE manufacturers and network equipment vendors to support such deployments. Rel-17, expected to be completed by 2022, and Rel-18, which is in the early study items approval stage at press time, will enhance the interworking and concrete use cases for interworking between 3GPP and non-3GPP networks and provide clarity around the converged core.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 796, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '44867fc68394e6a62935ca21e2ecad8d', 'text': 'Use of AI and ML in Securing 5G and Evolving Networks', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 796, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4503a033a8d2df85a15ba0adae8c0c9d', 'text': "Artificial intelligence (AI) and machine learning (ML) generally are used by vendors to showcase how their products are sophisticated and provide you with some “magic” and a cool user interface. Let's dig down a bit deeper and see what exactly AI and ML are and how to use them to secure your 5G and evolving technology deployments.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 796, 'parent\_id': '44867fc68394e6a62935ca21e2ecad8d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e963797379b1897df42eabc51e98131c', 'text': 'AI is the intelligence demonstrated by machines. AI was actually founded as an academic discipline in the 1955 and has since evolved to almost mimic human intelligence—of course, without emotions and consciousness.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 797, 'parent\_id': '44867fc68394e6a62935ca21e2ecad8d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e38941fabdefab4efd4909da169d85fc', 'text': 'ML is usually seen as a part of AI. ML is basically an algorithms model based on sampled data, also referred to as training data. ML algorithms make use of this sampled data to make certain decisions or predictions. The larger the set of training data, the more fine-tuned the algorithms become, and theoretical modeling can then be applied by AI to approximate and predict behavior.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 797, 'parent\_id': '44867fc68394e6a62935ca21e2ecad8d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e402ec65e83d8a86851eeeb052968faf', 'text': 'In the past, training an ML system was too computationally expensive. The improved availability of the CPUs and GPUs, the emergence of cloud computing, and the widespread use of open source big data technology such as Hadoop has massively reduced the price and encouraged rapid progress in the field of ML and eventually fine-tuned AI systems.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 797, 'parent\_id': '44867fc68394e6a62935ca21e2ecad8d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'ddcd7643a3d53f83346c4fcb39bca322', 'text': 'AI and ML are used in variety of applications, such as for research and development (R&D) teams in pharmaceutical industries to provide diagnoses to high-need areas such as cancer research, or in consumer-based areas such as human speech recognition systems in mobile phones and so on. The telecommunications industry will see more AI and ML adoption due to the deployment of 5G and upcoming technologies because of the massive amount of data that can now be collected to enhance various highly dense use cases, such as smart cities, which will see various types of IoT and M2M devices across different verticals, many of which need to coexist. One of the primary areas where AI and ML can be used is to enhance the security posture of your end-to-end networks. They can be used to identify any anomaly in the network and device behavior, decide if that anomalous behavior is malicious, and then mitigate it.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 797, 'parent\_id': '44867fc68394e6a62935ca21e2ecad8d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '11cd166ddf6efafca23ba821d1da7b0f', 'text': 'Applying innovative technologies like AI and ML on the collected data from 5G-capable devices, non-5G-capable devices, and network functions to proactively identify issues in the network such as predictive fault detection will be a key catalyst in ensuring full exploitation of the 5G technology within service providers and industry verticals adopting 5G by identifying anomalous behavior and making automated corrective actions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 797, 'parent\_id': '44867fc68394e6a62935ca21e2ecad8d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '05c9b07abebb820d7ff601aa3c4ffc13', 'text': 'To reduce human intervention and enhance the security posture of the network, you will require security automation that uses smart ML and AI. Traditionally, security automation is used for high-frequency tasks (in other words, tasks that have low-complexity and high-volume aspects of threat detection and mitigation). But for actual benefit in 5G systems, you need to have ML and AI', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 797, 'parent\_id': '44867fc68394e6a62935ca21e2ecad8d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd93622b120352d5442ba8a9d1ee93838', 'text': 'mechanisms that can proactively predict the threats with high accuracy based on the data collected from different parts of the 5G network.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 798, 'parent\_id': '44867fc68394e6a62935ca21e2ecad8d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '664365cddfd3c2477c25d19595420075', 'text': 'You can start building up the ML- and AI-based security posture by using service plane, management plane, and control plane information. Discussions with various service providers indicate that data collection on the user plane is not a priority, unless it is mandated by lawful entities based on the country or for specific IoT use cases. IoT use cases will require careful implementation of security controls to ensure that bot-based attacks do not cause a denial of service (DoS) for your legitimate users.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 798, 'parent\_id': '44867fc68394e6a62935ca21e2ecad8d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3956c513bb0cebf3e8f975db10f117e3', 'text': 'Figure 12-6 illustrates the use of AI and ML to enhance the security posture in your 5G and evolving technology deployments.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 798, 'parent\_id': '44867fc68394e6a62935ca21e2ecad8d', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Image', 'element\_id': 'a1e731e852d108d36bc17da94e3cf593', 'text': '— Constant monitoring to identify behavioral anomalies Threat Intel — Predictive Algorithms to predict zero-day atiacks gL — | Anomaly Detection Al Platform > |dentify suspicious activity in public cloud deployed apps > |dentify malware in encrypted traffic without decryption Technology Vendor Data Collection e/ y hosted public cloud ) ~ ((A)) Multi-RAT Wired, 4G, 5G, 6G NFs 3GPP Access 0C Infra @ @ Pubhc Cloud ’ w | J (((@ D = \_ S~~~ Providert o 1 - WiFi/WLC 3GPP Mult-RAT and non-3GPP Non-3GPP Access Wireline and Wireless Converged Core ¢ Public Cloud Provider 2', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 799, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b37748fa06f896531a8bc0aee5fbb17a', 'text': 'Figure 12-6 Example of Using AI and ML to Enhance Your Security Posture', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 799, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '028a7991a0b5cd7117fbbe3955b8d940', 'text': 'As shown in Figure 12-6, AI and ML detect threats by constantly monitoring the behavior of the new and legacy networks, including public cloud–based network function deployments, for any anomalies. Machine learning engines process massive amounts of data in near real time, which will help you discover critical incidents in critical use cases such as critical infrastructure and smart city use cases. These techniques also allow for the detection of insider threats, unknown malware, and policy violations to improve the infrastructure security.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 799, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '4138c2de961e80c51f259893fc2c38c3', 'text': 'In a constantly changing threat landscape, you need to ensure that the vendors you select use AI and ML to support comprehensive, automated, coordinated responses between various security components.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 800, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b3a4ed750be16e121ab96db2bdd5870b', 'text': "5G and evolving architectures enable you to provide use cases that define true digital transformation. Use cases such as vehicle-to-everything (V2X), where the vehicle communicates with other cars, pedestrian systems, multi-radio access networks, and sensors to optimize traffic speed will require security capabilities to ensure that attackers don't disrupt the networks and cause chaos. In critical use cases such as the energy and water sectors, gathering data from various sensors and running it through an AI- and ML-based security system will ensure smooth operation and mitigate any threats by detecting and understanding any anomalies in device behavior, thereby enabling proactive, preventive maintenance to eliminate downtime.", 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 800, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '26c1c537cd39fe0d37c53ab6147e01c5', 'text': 'Crypto Agility in 5G and Evolving Technologies', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 800, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '148e1beb1931e8019cdfbe68c16809c8', 'text': 'The term crypto agility refers to the ability of an organization to swiftly shift from existing cryptographic technology to newer, more robust ones. Crypto agility is very important if you plan to deploy millions of IoT devices, many of which depend on the non-3GPP network to connect to the 3GPP network. With quantum computing becoming more popular, several popular public-key cryptography systems such as RSA could be broken.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 800, 'parent\_id': '26c1c537cd39fe0d37c53ab6147e01c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd8fc212cd9933753e04b3c2f6f319817', 'text': 'The reason existing asymmetric crypto algorithms are vulnerable to quantum computing is due to the fact that they rely on large, universal quantum computers that can compute on a very large scale and solve the integer factorization and discrete log problems used by RSA, Diffie-Hellman (DH), and so on at a much faster rate than usual computers. For symmetric algorithms, the impact is less severe, but the effective key length is at most halved. In other words, this new generation of quantum computers will solve mathematical tasks much faster than existing computers. This means that an attacker with a quantum computer can obtain a private key from a corresponding public key, rendering PKI deployment, which is used in security protocols such as Transport Layer Security (TLS), ineffective with current cryptographic algorithms such as RSA, DH, and so on.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 800, 'parent\_id': '26c1c537cd39fe0d37c53ab6147e01c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'a6290e4b941468798b3b41428e6629b9', 'text': 'When this will happen, though not clear, is actually just a matter of time. To mitigate such occurrences, you should identify the best options and plan to move your public key systems toward post-quantum-cryptography systems', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 800, 'parent\_id': '26c1c537cd39fe0d37c53ab6147e01c5', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'd9d00c6eef6c90d4c0f7fdbeb508aeb6', 'text': '(such as Lattice) at least for the devices in untrusted networks connecting to your 3GPP network. This is important for use cases such as massive IoT (mIoT) and machine-to-machine (M2M), where you might need to cater for millions of devices, as many of these devices use cryptographic algorithms that are not quantum safe.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 801, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7c1d48cbe38285291b181ec99f22bf8d', 'text': 'Here are some key practical considerations you should take before moving to a fully quantum safe cryptographic state (FQSCS):', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 801, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '76cd4ae57935163003e34b6bb1105911', 'text': '• Prepare an inventory of the cryptographic algorithms used in your IT and telco environment. This can be done using scanning or monitoring solutions.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 801, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'fc257108c2efb13646750bd4d73b44e6', 'text': '• Identify the parts of your network that could be susceptible to attacks, such as critical infrastructures, and ensure that you prioritize those network components for migration toward FQSCS. This can be done using end-to- end enhanced visibility solutions that show you the network topology of your 5G network, helping you determine the most exposed and vulnerable parts of your critical infrastructure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 801, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '8a7e2ed1352870b5a1f7562da3bad15b', 'text': '• Identify and understand the security properties of the quantum-safe cryptographic algorithms and protocols.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 801, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '121cd65548e41ac4fcd61de30cf48318', 'text': '• Identify whether the quantum-safe cryptographic algorithm (QSCA) you plan to implement requires being validated by industry efforts like the Cryptographic Module Validation Program (CMVP). CMVP is a joint effort between the National Institute of Standards and Technology, under the Department of Commerce, and the Canadian Centre for Cyber Security. The goal of the CMVP is to promote the use of validated cryptographic modules and provide federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 801, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '50352342b5d1199f87e48ff5972c1a6b', 'text': '• Validate the compatibility and impact of quantum-safe cryptographic algorithms in your existing architectures. Identify parts of your 5G network and use cases that are dependent on low latency. This can be done by checking the number of network slices configured for your 5G network, which is usually configured in your 5G Core (5GC), and then identifying the slices that are dependent on latency. For example, a vehicle-to-everything (V2X) slice is deemed to be an ultra-reliable low- latency communication (URLLC) use case that is highly dependent on', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 801, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '868abaef72ae8e216aebb0b3c942e926', 'text': 'latency. Any increase in latency for such use cases can cause service disruption.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 802, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3f4bdd75003c3664d346aaaef71f6567', 'text': '• Consider the compatibility and impact of quantum-safe cryptographic algorithms in security offerings for industry vertical use cases. This can be determined by having discussions with your 5G slice consumers and identifying whether their network devices can implement QSC algorithms.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 802, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '399ce32588bcfaf56f71c61e8b2b548c', 'text': '• Consider the cost of switching to quantum-safe cryptographic algorithms.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 802, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'b15019c71055e1ae1da6b1240b72b298', 'text': 'The European Telecommunications Standards Institute (ETSI) published a report, TR 103.619, that defines the migration strategies and recommendations for quantum-safe schemes and enhancing cryptography awareness. ETSI recommends three stages for your infrastructure to migrate to FQSCS:', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 802, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '31447ccaa9d2190dd170eab59b29c4d1', 'text': '• Stage 1: Aimed at compiling all inventories and identifying business process requirements.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 802, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e1328a2cf6abf914f17efa5f1d833140', 'text': '• Stage 2: Caters for preparation of the migration plan, including the hardware-based security environment, key management, isolation of the sub-systems involved in migration, and business processes to enable execution of the migration.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 802, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'e44a407b45daf6856067bba23a469fce', 'text': '• Stage 3: Caters for execution of the migration.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 802, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '698fbffd17264153481fefba355a8231', 'text': 'The National Institute of Standards and Technology (NIST) has also initiated a process to identity, evaluate, and standardize post-quantum cryptography (PQC) algorithms.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 802, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '91b26bb4559b71361d13557dbb2a5f61', 'text': 'Other methods to make 5G and evolving technology deployments crypto-agile include ensuring automation of digital certificates and private key rotations as well as implementing hash algorithms with different lengths of output. If a vulnerability is found in the quantum-safe cryptographic algorithm, it might be necessary to switch to a different quantum-safe algorithm entirely, although in some instances the specific vulnerability can be addressed by restricting modes or by revising the strength of individual parameters. Ensuring cryptographic agility will make this significantly easier.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 802, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '6f5577c4f81fd8344779eaf4e6cd3403', 'text': 'Ensure that all the members of your security team, from security strategy to the application development engineers, understand the need for crypto-agile implementation; it should be taken into consideration for each and every strategy, design, product, and deployment decision.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 802, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f0d7b7ffdc86574b0754915297d6ac12', 'text': 'You should also focus on some key methods, such as ensuring that your network equipment and device vendors supply you with the most recent cryptographic protocols and algorithms. They should also supply you with software updates and provide you with information on crypto agility of the hardware and software used in their products.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 803, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '2feb01ea9fc145cbc7db53115c48af38', 'text': 'Summary', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 803, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7fb05d7e7684bc2ed9408190bb53650f', 'text': 'Migrating to 5G SA and adapting it for various 5G-related use cases requires the right security controls and best practices. Although 3GPP will provide enhancements in Rel-17 and upcoming specifications, it will not be enough for the wider 5G ecosystem to be secure—the main reason being the integration of 3GPP-specified systems with other non-3GPP systems. Although there is on- going work in these areas, the work is in the early stages and requires further development, and the technology partner ecosystem needs to be widened.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 803, 'parent\_id': '2feb01ea9fc145cbc7db53115c48af38', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '816b2dc667dcf965349ae674f6ffa638', 'text': 'You will also need to use AI and ML systems for your network for variety of security use cases. The security posture of your network can benefit from AI and ML, as they enable near-real-time detection of threats, prediction of possible zero-day attacks, identification of anomalies in the network, and mitigation of threats.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 803, 'parent\_id': '2feb01ea9fc145cbc7db53115c48af38', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f88506df4a413e99f955db6e9a4ae9b4', 'text': 'It is also very important to provide crypto agility to your network to ensure that you can adopt newer, more robust cryptographic algorithm systems. This will help better secure your network and devices from advanced persistent threats (APTs) and take you toward the next step of getting your network to a fully quantum-safe cryptographic state (FQSCS).', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 803, 'parent\_id': '2feb01ea9fc145cbc7db53115c48af38', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '0658cba134c1ecbeb345ac42a55e8bc6', 'text': 'All these different discussions bring us to the conclusion that we need to look at security from a different angle and secure converging technologies and integrations that allow flexible deployments and an open ecosystem.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 803, 'parent\_id': '2feb01ea9fc145cbc7db53115c48af38', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'bce4a9530cc7cd4baad3acf0ac25502e', 'text': 'As the network evolves, opening up and bringing in the deployment of mobile packet core network functions within the public cloud and closer third-party application integrations, the cybersecurity controls also need to evolve to ensure your infrastructure remains protected to keep the sensitive data of your employees, subscribers and customers secure.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 803, 'parent\_id': '2feb01ea9fc145cbc7db53115c48af38', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': 'adaadef0a8540d5528061fea09b9cec4', 'text': 'Acronym Key', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 803, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '3cf97fc33eb52c76ca97df7640383c6a', 'text': 'The following table expands the key acronyms used in this chapter.', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 804, 'parent\_id': 'adaadef0a8540d5528061fea09b9cec4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '7c8ae1b0c8d9cdc2ec6af7e318de79f5', 'text': 'Acronym Expansion 5GC 5G Core Network AMF Access and Mobility Function API Application programming interface AUSF Authentication Server Function CNF Cloud-Native Function FQSCS Fully quantum-safe cryptographic state IAM Identity and Access Management loT Internet of Things M2M Machine-to-machine MBB Mobile broadband MEC Multi-access edge compute N3IWF Non-3GPP Inter-Working Function N5SCW Non-5G-capable over WLAN NSGC Non-5G-capable NEF Network Exposure Function NF Network Function NSaaS Network slice as a service NSSF Network Slice Selection Function PKI Public key infrastructure QSC Quantum-safe cryptography RAT Radio access technology', 'metadata': {'text\_as\_html': '<table><thead><tr><th>Acronym</th><th>Expansion</th></tr></thead><tbody><tr><td>5GC</td><td>5G Core Network</td></tr><tr><td>AMF</td><td>Access and Mobility Function</td></tr><tr><td>API</td><td>Application programming interface</td></tr><tr><td>AUSF</td><td>Authentication Server Function</td></tr><tr><td>CNF</td><td>Cloud-Native Function</td></tr><tr><td>FQSCS</td><td>Fully quantum-safe cryptographic state</td></tr><tr><td>IAM</td><td>Identity and Access Management</td></tr><tr><td>loT</td><td>Internet of Things</td></tr><tr><td>M2M</td><td>Machine-to-machine</td></tr><tr><td>MBB</td><td>Mobile broadband</td></tr><tr><td>MEC</td><td>Multi-access edge compute</td></tr><tr><td>N3IWF</td><td>Non-3GPP Inter-Working Function</td></tr><tr><td>N5SCW</td><td>Non-5G-capable over WLAN</td></tr><tr><td>NSGC</td><td>Non-5G-capable</td></tr><tr><td>NEF</td><td>Network Exposure Function</td></tr><tr><td>NF</td><td>Network Function</td></tr><tr><td>NSaaS</td><td>Network slice as a service</td></tr><tr><td>NSSF</td><td>Network Slice Selection Function</td></tr><tr><td>PKI</td><td>Public key infrastructure</td></tr><tr><td>QSC</td><td>Quantum-safe cryptography</td></tr><tr><td>RAT</td><td>Radio access technology</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 804, 'parent\_id': 'adaadef0a8540d5528061fea09b9cec4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Table', 'element\_id': '19e8db51cf8832aa05bd1f9310b567ff', 'text': 'SBA Service-based architecture SBI Service-based interface SEAF Security Anchor Functionality SEPP Security Edge Protection Proxy SMF Session Management Function SUCI Subscription Concealed Identifier SUPI Subscription Permanent Identifier TLS Transport Layer Security TNAN Trusted Non-3GPP Access Network TNAP Trusted Non-3GPP Access Point TNGF Trusted Non-3GPP Gateway Function TNL Transport Network Layer TWAP Trusted WLAN Access Point TWIF Trusted WLAN Interworking Function UDM Unified Data Management UPF User Plane Function UPF User Plane Function VNF Virtual Network Function VNFM Virtual Network Function Manager W-5GAN Wireline 5G Access Network W-5GBAN Wireline BBF Access Network W-5GCAN Wireline 5G Cable Access Network W-AGF Wireline Access Gateway Function WAF Web application firewall', 'metadata': {'text\_as\_html': '<table><thead><tr><th>SBA</th><th>Service-based architecture</th></tr></thead><tbody><tr><td>SBI</td><td>Service-based interface</td></tr><tr><td>SEAF</td><td>Security Anchor Functionality</td></tr><tr><td>SEPP</td><td>Security Edge Protection Proxy</td></tr><tr><td>SMF</td><td>Session Management Function</td></tr><tr><td>SUCI</td><td>Subscription Concealed Identifier</td></tr><tr><td>SUPI</td><td>Subscription Permanent Identifier</td></tr><tr><td>TLS</td><td>Transport Layer Security</td></tr><tr><td>TNAN</td><td>Trusted Non-3GPP Access Network</td></tr><tr><td>TNAP</td><td>Trusted Non-3GPP Access Point</td></tr><tr><td>TNGF</td><td>Trusted Non-3GPP Gateway Function</td></tr><tr><td>TNL</td><td>Transport Network Layer</td></tr><tr><td>TWAP</td><td>Trusted WLAN Access Point</td></tr><tr><td>TWIF</td><td>Trusted WLAN Interworking Function</td></tr><tr><td>UDM</td><td>Unified Data Management</td></tr><tr><td>UPF</td><td>User Plane Function</td></tr><tr><td>UPF</td><td>User Plane Function</td></tr><tr><td>VNF</td><td>Virtual Network Function</td></tr><tr><td>VNFM</td><td>Virtual Network Function Manager</td></tr><tr><td>W-5GAN</td><td>Wireline 5G Access Network</td></tr><tr><td>W-5GBAN</td><td>Wireline BBF Access Network</td></tr><tr><td>W-5GCAN</td><td>Wireline 5G Cable Access Network</td></tr><tr><td>W-AGF</td><td>Wireline Access Gateway Function</td></tr><tr><td>WAF</td><td>Web application firewall</td></tr></tbody></table>', 'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 805, 'parent\_id': 'adaadef0a8540d5528061fea09b9cec4', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'Title', 'element\_id': '5279fc078168ae7caa0c387a65367906', 'text': 'References', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 806, 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '06db3cab692213c34c1d70e8d6d72daf', 'text': '3GPP TS 23.501, “System Architecture for the 5G System: Stage 2” 3GPP TS 33.501, “Security Architecture and Procedures for 5G System”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 806, 'parent\_id': '5279fc078168ae7caa0c387a65367906', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': 'f39bd751d457f2cbb2efaf8bf1022894', 'text': '3GPP TR 103.619, “Migration strategies and recommendations to Quantum Safe schemes”', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 806, 'parent\_id': '5279fc078168ae7caa0c387a65367906', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '05a085b1fee7c0868ea61b5ffb264ad2', 'text': 'Cisco Systems, “Transforming Business with Artificial Intelligence,” Cisco Public, 2018', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 806, 'parent\_id': '5279fc078168ae7caa0c387a65367906', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '7f2a02e014d93012e14fa0e44a992467', 'text': 'Cisco Systems, “Reimagining End-to-End Network Mobile Network,” Cisco Public, 2019', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 806, 'parent\_id': '5279fc078168ae7caa0c387a65367906', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '85961a7b29b6b71e126c04fe35d3171c', 'text': 'https://www.itu.int/en/ITU-', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 806, 'parent\_id': '5279fc078168ae7caa0c387a65367906', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '9cb1da69f0cdd79f7f7658935d60ebab', 'text': 'T/focusgroups/net2030/Documents/White\_Paper.pdf', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 806, 'parent\_id': '5279fc078168ae7caa0c387a65367906', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}

{'type': 'NarrativeText', 'element\_id': '36113d0e1b5c2da8539b779caab7ddcb', 'text': 'https://www.3gpp.org/specifications/67-releases', 'metadata': {'filetype': 'application/pdf', 'languages': ['eng'], 'page\_number': 806, 'parent\_id': '5279fc078168ae7caa0c387a65367906', 'filename': 'Securing 5G and Evolving Architectures -- Pramod Nair -- 1, 2021 -- Addison-Wesley Professional -- 9780137457939 -- ec1c459557ba330c3cda0333f796d0ed -- Anna’s Archive.pdf'}}