A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions

Chamitha De Alwis, *Senior Member, IEEE*, Pawani Porambage, *Senior Member, IEEE*, Kapal Dev, *Senior Member, IEEE*, Thippa Reddy Gadekallu, *Senior Member, IEEE*, and Madhusanka Liyanage, *Senior Member, IEEE*

***Abstract*—The dawn of softwarized networks enables Network Slicing (NS) as an important technology towards allocating end-to-end logical networks to facilitate diverse requirements of emerging applications in fifth-generation (5G) mobile networks. However, the emergence of NS also exposes novel security and privacy challenges, primarily related to aspects such as NS life-cycle security, inter-slice security, intra-slice security, slice broker security, zero-touch network and management security, and blockchain security. Hence, enhancing NS security, privacy, and trust has become a key research area toward realizing the true capabilities of 5G. This paper presents a comprehensive and up-to-date survey on NS security. The paper articulates a taxonomy for NS security and privacy, laying the structure for the survey. Accordingly, the paper presents key attack scenarios specific to NS-enabled networks. Furthermore, the paper explores NS security threats, challenges, and issues while elaborating on NS security solutions available in the literature. In addition, NS trust and privacy aspects, along with possible solutions, are explained. The paper also highlights future research directions in NS security and privacy. It is envisaged that this survey will concentrate on existing research work, highlight research gaps and shed light on future research, development, and standardization work to realize secure NS in 5G and beyond mobile communication networks.**

***Index Terms*—Network slicing, network security, network softwarization, privacy, trust, 5G security.**

Manuscript received 1 December 2022; revised 14 May 2023 and 9 July 2023; accepted 16 August 2023. Date of publication 6 September 2023; date of current version 27 February 2024. This work was supported in part by European Union through SPATIAL Project under Grant 101021808, through CONFIDENTIAL-6G Project under Grant 101096435, and in part by the Science Foundation Ireland through CONNECT Phase 2 Project under Grant 13/RC/2077_P2. *(Corresponding author: Madhusanka Liyanage.)*

Chamitha De Alwis is with the School of Computer Science and Technology, University of Bedfordshire, LU1 3JU Luton, U.K. (e-mail: chamitha@ieee.org).

Pawani Porambage is with the VTT Technical Research Centre of Finland, 90570 Oulu, Finland (e-mail: pawani.porambage@vtt.fi).

Kapal Dev is with the CONNECT Centre and the Department of Computer Science, Munster Technological University, Cork, T12 P928 Ireland, also with the Institute for Intelligent Systems, University of Johannesburg, Johannesburg 2092, South Africa, and also with the Department of Electrical and Computer Engineering, Lebanese American University, Byblos, Lebanon (e-mail: kapal.dev@ieee.org).

Thippa Reddy Gadekallu is with the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore 632014, India, also with the Department of Electrical and Computer Engineering, Lebanese American University, Byblos, Lebanon, also with the Research and Development Department, Zhongda Group, Jiaxing 314312, Zhejiang, China, also with the College of Information Science and Engineering, Jiaxing University, Jiaxing 314001, China, and also with the Division of Research and Development, Lovely Professional University, Phagwara 144001, India (e-mail: thippareddy.g@vit.ac.in).

Madhusanka Liyanage is with the School of Computer Science, University College Dublin, Dublin 4, D04 V1W8 Ireland (e-mail: madhusanka@ucd.ie).

Digital Object Identifier 10.1109/COMST.2023.3312349

I. Introduction

THE ADVENT of the fifth generation (5G) mobile networks has enabled a plethora of diverse applications ranging from Virtual Reality (VR), Augmented Reality (AR), and Connected Autonomous Vehicles (CAV) to the Internet of Everything (IoE) [1]. These applications are enabled through enhanced Mobile BroadBand (eMBB), ultra Reliable Low Latency Communication (uRLLC), and massive Machine Type Communication (mMTC) features of 5G. eMBB enables data rates up to 10 Gbps, uRLLC allows End-to-End (E2E) latencies below 1 ms, and mMTC facilitates up to 1,000,000 connected devices/km^2 [2], [3]. Furthermore, 5G network reliability and availability are also expected to exceed 99.999% [2]. Realizing such advanced and diverse 5G features is not feasible through fixed and inflexible conventional network infrastructures [4]. Thus, 5G introduces a flexible, agile, dynamic, and programmable network architecture through network softwarization [4], [5].

The evolution of networks from conventional networks to softwarized networks towards realizing efficient, flexible, scalable, and high-performance networks is illustrated in Fig. 1 [4]. Accordingly, major milestones towards network softwarization are network virtualization and cloudification, service migration, orchestration of networks and services, and automation of network services [4]. Network virtualization banks on three major technologies, namely, Software Defined Networking (SDN), Network Function Virtualization (NFV), and cloud computing [6], [7]. SDN separates the control plane and the data plane of networks where the network infrastructure can be abstracted, programmed, and controlled through softwarized network functions [8]. These softwarized network functions are decoupled from proprietary networking hardware by NFV to run the network functions as software instances in virtual machines [9]. Such virtual machines catering to network elements and network functions can be hosted in the cloud through network cloudification [10]. Following network cloudification, network services are migrated towards the cloud [11], [12]. Furthermore, network functions are orchestrated to synchronize E2E network operations and ensure the smooth and efficient functioning of mobile networks [5]. In addition, network operations and services are automated through technologies such as Multi-access Edge Computing (MEC) and Network Slicing (NS) [4]. MEC extends cloud computing towards the Radio Access Network (RAN) edge to provide real-time access to radio network resources [13]. NS,

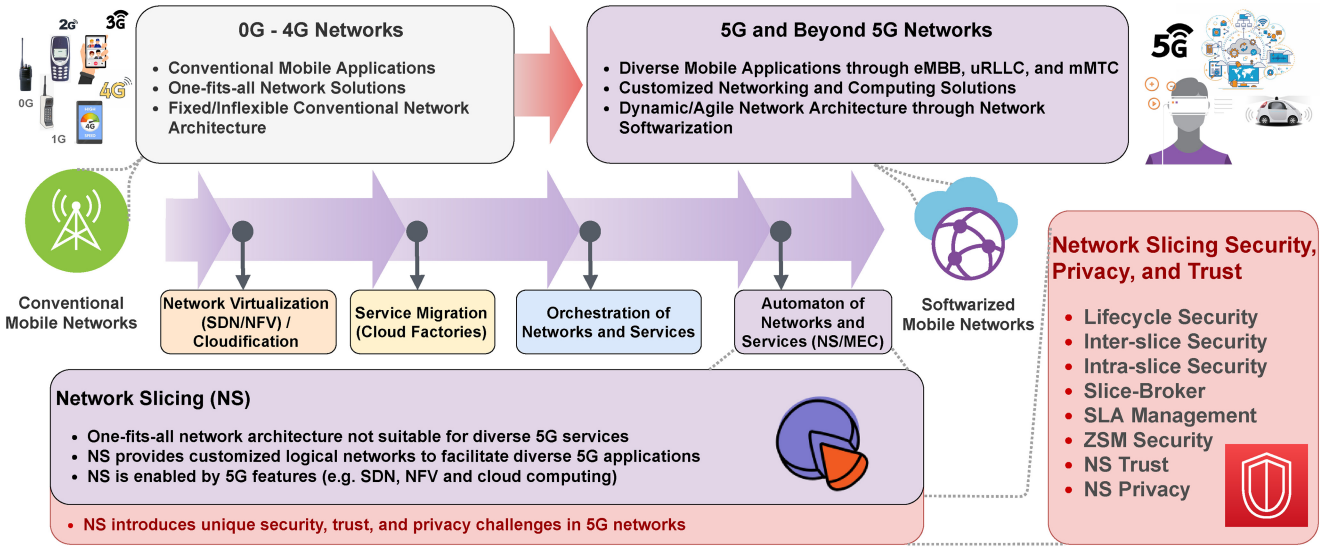

Fig. 1. Evolution of network softwarization towards network slicing security, privacy, and trust [4], [6].

TABLE I
SUMMARY OF IMPORTANT ACRONYMS

Acronym	Definition
5G	Fifth Generation mobile networks
6G	Sixth Generation mobile networks
AI	Artificial Intelligence
AR	Augmented Reality
API	Application Programming Interfaces
DDoS	Distributed Denial-of-Service
DLT	Disrtibuted Ledger Technology
DoS	Denial-of-Service
MBB	Mobile Broadband
CAV	Connected Autonomous Vehicles
CN	Core Network
E2E	End-to-End
eMBB	enhanced Mobile BroadBand
IoE	Internet of Everything
MANO	Management and Orchestration
MEC	Multi-access Edge Computing
ML	Machine Learning
mMTC	massive Machine Type Communication
NF	Network Function
NFV	Network Function Virtualization
NS	Network Slicing
NSaaS	Network Slicing as a Service
PbD	Privacy by Design
RAN	Radio Access Network
SbD	Security by Design
SDN	Software Defined Networking
SLA	Service Level Agreement
SSLA	Security Service Level Agreement
uRLLC	ultra Reliable Low Latency Communication
VNF	Virtualized Network Function
VR	Virtual Reality
ZSM	Zero touch network and management systems

on the other hand, configures network functions such that it can allocate end-to-end logical networks identified as "network slices". These network slices ensure that mobile networks can facilitate diverse network requirements of 5G applications. Hence, NS is considered as one of the most important 5G technologies that play a significant role in enabling emerging 5G applications [14], [15].

A. Network Slicing

5G networks are expected to be revolutionary compared with their predecessors, not only due to the enhanced connectivity it offers but also due to the support for diverse 5G services [14], [16]. Thus, besides numerous network and application optimizations [17], [18], [19], [20], the "one-fits-all" network architecture of the pre-5G networks are not suitable to provide 5G applications and services [21], [22], [23], as highlighted in Fig. 1. Hence, 5G network architecture is designed to be dynamic and agile through network softwarization [24]. The Next Generation Network Alliance (NGMN) announced the concept of NS in 2015 as an important step towards realizing softwarized networks [25]. Both 3GPP and 5G-PPP proposed 5G architectures also consider NS as an important enabler of softwarized 5G networks [26], [27]. NS is enabled by three main softwarized network features: SDN, NFV, and cloud computing [6]. NS enables different verticals to coexist over the same physical network infrastructure by running multiple logical networks by creating E2E network slices across the RAN and the Core Network (CN). A network slice is designed of Network Functions (NFs) and Virtualized Network Functions (VNFs) tailored to offer network capabilities towards facilitating specific applications and use-cases [28].

B. Network Slicing Security and Privacy

The development of NS as a mainstream technology utilized in 5G networks requires addressing many research challenges including efficient network resource utilization for NS, slice management and orchestration, development of NS business models, and ensuring network security and privacy with NS [41]. 5G and beyond 5G networks expose novel security and privacy vulnerabilities with the emergence of NS as a key technology towards softwarized networks [42]. Any security or privacy vulnerability in the NS architecture can result in security and privacy attacks that would result in issues such as data breaches, and network and other service disruptions.

Therefore, ensuring NS security and privacy in 5G and beyond 5G networks is paramount.

Primarily, NS-related security issues can be discussed under LC Security, Inter-Slice Security, and Intra-Slice Security [43]. For instance, the Life Cycle (LC) of a Network Slice Instance (NSI) may span across multiple networks, virtual infrastructures, and data centers. This may give rise to multiple security and privacy threats such as impersonation attacks, identity thefts, privacy attacks, Denial-of-Service (DoS)/Distributed Denial-of-Service (DDoS) attacks, traffic, and data modification, and unauthorized access [6]. Furthermore, inter-slice security is concerned with security concerns between multiple slices while intra-slice security deals with security issues within a network slice. Therefore, solid measures and precautions should be taken to ensure the security of NS in softwarized 5G and beyond networks.

Strong isolation between network slice instances is one of the key requirements to ensure NS security. Slice isolation requires no influence between network slices or any related entities within a slice including NFs and users [29]. Slice isolation should be considered throughout the network including in hypervisors, operating systems, network hardware, network operators, and Application Programming Interfaces (API). Furthermore, strong encryption, authentication, access control, and physical protection techniques can be utilized to ensure NS security.

NS also inherits security and privacy threats due to the dependence on SDN, NFV, and cloud computing. In addition, NS security solutions can be extended towards advanced solutions such as AI/ML-based solutions, security orchestration, blockchain-based solutions, Security Service Level Agreement (SSLA) policy management, and Security by Design (SbD) [29], [43]. Furthermore, as tenants in NS utilize common resources, an information leak may give rise to privacy violations. This is evident when NS is used for IoT applications that deal with high-volume data sets [44]. Addressing this type of concern require strong privacy isolation using privacy rules and adhering to privacy concepts such as Privacy by Design (PbD) [43], [45]. In addition, trust-related issues in NS can be addressed through blockchain/Distributed Ledger Technology (DLT) based solutions while Artificial Intelligence (AI) enabled NS trust issues can be addressed through a trust broker [46], [47].

C. Paper Motivation

Considering that NS is envisaged to play a significant role in 5G and beyond networks, several research work have discussed NS-related security and privacy issues. However, non of the existing work provides a comprehensive discussion on NS, covering aspects ranging from NS security and privacy attacks, threats, challenges, issues, solutions, and research directions, as evident in TABLE II. For instance, [15] presents NS security challenges at the packet core, solutions, and possible directions. Yet, the scope is limited while security aspects are not discussed comprehensively. Furthermore, [6] provides a discussion on NS security threats, vulnerabilities, and mechanisms. However, the scope of this work is limited as security threats, solutions, and privacy aspects are not discussed. In addition, [29] discusses NS security in 5G highlighting available threats and providing recommendations. This paper also highlights some open security challenges related to NS. However, the scope of this work is limited to only life-cycle security, intra-slice security, and inter-slice security. Also, [30] provides a concise discussion on NS with a limited focus on security challenges, solutions, and merits of NS. Furthermore, [21] explores NS towards realizing IoT, which does not provide a comprehensive overview of NS security aspects. Also, [4] focuses on the security and privacy aspects of 5G technologies, which does not provide a detailed view of security and privacy aspects specific to NS. Moreover, [31] surveys end-to-end 5G NS models but does not extensively discuss NS security aspects. The work presented in [32] focuses on network softwarization, NS principals, and technologies. Furthermore, [33] focuses on 5G NS architecture and challenges, while [34] surveys network virtualization hypervisors for SDN. In addition, [35] surveys prospective technologies for 6G security and privacy while the focus on NS security and privacy is limited. Likewise, [36] surveys multi-access edge computing security and privacy with a limited focus on NS security. The work presented in [37] focuses on network security opportunities and challenges in software-defined mobile networks. Furthermore, [38] provides a vision on 6G security and privacy, where the discussion on security aspects related to NS is limited. In addition, [39] focuses on ML base NS concepts, threats, and attacks. A summary of these work are provided in TABLE II.

According to TABLE II, the existing literature only provides a limited discussion on NS security and privacy aspects. Furthermore, the content related to NS security and privacy is largely overlapping and only provides a high-level overview. Moreover, many aspects, including, NS attack scenarios, detailed discussion on NS security solutions, detailed threat taxonomy, comprehensive analysis of NS trust and privacy, and an in-depth discussion on the lessons learned and future work related to NS security and privacy, is hardly covered in the existing literature.

Therefore, as highlighted in TABLE II, there exists a significant void for a comprehensive and up-to-date literature survey to facilitate research, development and standardization work towards establishing a secure NS framework in 5G and beyond networks. In response, this paper provides a comprehensive analysis of all aspects related to NS security and privacy, which is both timely and essential for securing future mobile communication networks.

D. Paper Contribution

This paper focuses on providing a comprehensive and up-to-date review of NS security and privacy. To the best of the authors' knowledge, this is the first attempt to comprehensively survey NS attacks, NS security threats/challenges/issues, NS security solutions, NS trust and privacy, and research directions related to NS security and privacy. The main contributions of this survey are listed below.

TABLE II
SUMMARY OF IMPORTANT SURVEYS ON NETWORK SLICING SECURITY AND PRIVACY

Ref.	NS Attack Scenarios	NS Security Threats/Challenges/Issues	NS Security Solutions	NS Trust and Privacy	NS Security/Privacy Future Directions	Remarks
[6]	L	H	M	L	M	NS security threats and vulnerabilities are explained elaborating the need for strong slice isolation. However, the scope of this is limited and many security threats, solutions, and privacy aspects are not discussed.
[15]	L	M	L	L	L	The paper provides a brief discussion focusing on some NS security aspects. However, the scope is limited and security aspects are not discussed comprehensively.
[29]	L	H	M	L	M	This work focuses only on life-cycle security, intra-slice security, and inter-slice security. Other remaining security aspects and privacy aspects are not discussed.
[30]	L	L	M	L	L	This is a concise discussion about NS security in a limited scope.
[31]	L	L	L	L	L	This work surveys on E2E 5G NS model and NS security aspects are not discussed extensively.
[32]	L	M	L	L	L	This work focuses on network softwarization, NS principals, and technologies. The discussion on NS security is limited.
[33]	L	L	L	L	L	This work focuses on 5G NS architecture and challenges. The focus on NS security is limited.
[34]	L	L	L	L	L	This work surveys network virtualization hypervisors for SDN. The discussion on NS security aspects are not discussed.
[35]	L	L	L	L	L	This paper surveys prospective technologies for 6G security and privacy. The discussion on NS security and privacy is limited.
[21]	L	M	M	M	L	This paper surveys the applicability of NS towards realizing Internet of Things applications in 5G networks. Some NS security solutions and privacy concerns are discussed.
[36]	L	M	M	L	M	This paper surveys multi-access edge computing security and privacy. Provides a brief discussion on NS security issues, solutions and future directions.
[37]	L	L	L	L	L	This paper focuses on network security opportunities and challenges in software defined mobile networks. This paper does not discuss on NS specific security and privacy.
[38]	L	L	L	L	L	This paper provides a vision on 6G security and privacy. The discussion on security aspects related to NS is limited.
[4]	L	M	M	L	L	This paper discusses security and privacy solutions and future directions of 5G technologies. Discusses some security issues and solutions.
[39]	M	M	M	L	M	This paper focuses on ML base NS concepts, threats, and attacks.
[40]	M	H	H	L	L	This paper presents a review on some NS security issues and solutions. However, the scope is limited as many attacks, threats, solutions and future research directions have not been discussed in detail.
This Survey	H	H	H	H	H	This paper presents a comprehensive survey spanning from NS threat model and taxonomy, NS security threats and challenges, NS security solutions, NS trust and privacy, NS projects, SDO activities, and future research directions.

L No information or explores the area briefly M Provides some information about the area H Explores the area in detail

- *Propose a Taxonomy for NS Security and Privacy:* This work provides a comprehensive and up-to-date taxonomy for NS security and privacy.
- *Explore NS attacks:* This paper provides a detailed overview on key attack scenarios in NS, ranging from location-tracking attacks to side-channel attacks.
- *Present NS threats, and security and privacy goals:* The paper models NS threats and presents a threat taxonomy while elaborating on NS security and privacy goals.
- *Elaborate NS security threats, challenges, and issues:* The paper elaborates on NS security threats, security challenges and prevailing issues.
- *Formulate NS security solutions:* The paper explains NS security solutions ranging from AI/ML-based solutions to introducing dedicated security slices for improving network security.
- *Discuss NS trust and privacy:* NS trust and privacy aspects and possible solutions are explained.
- *Articulate future research directions:* The paper proposes future directions considering the lessons learned throughout the existing developments of NS security and privacy.

E. Paper Outline

The rest of the paper is organized as follows. Section II presents the NS concept and proposes a taxonomy for NS security. Section III presents various attack scenarios that can

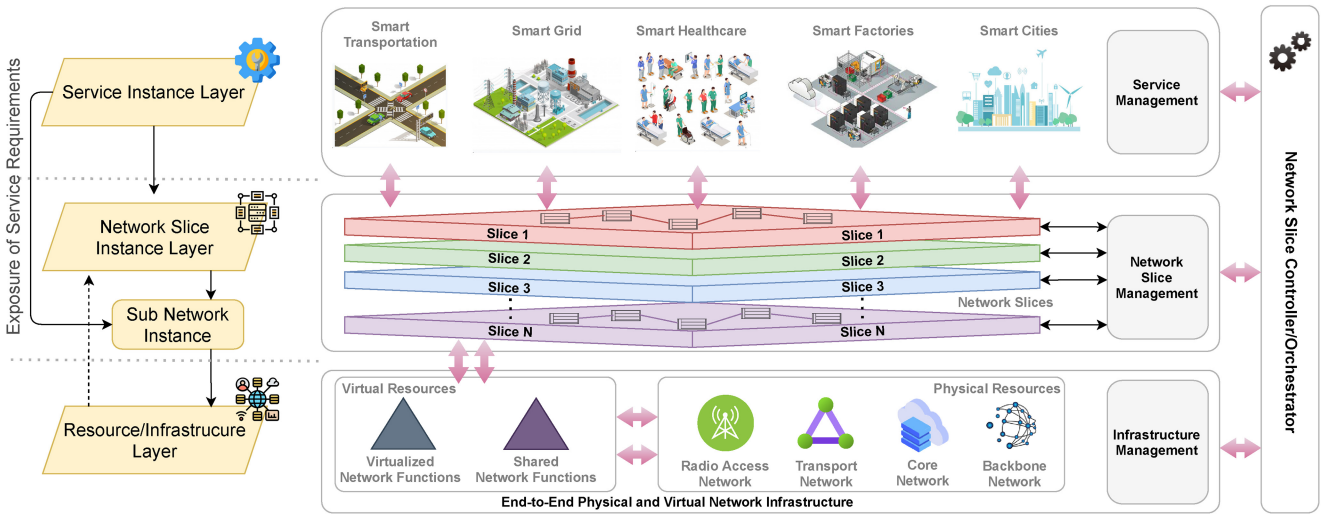

Fig. 2. Network Slicing Architecture.

be performed against NS. NS security threats, challenges, and issues are discussed in Section IV while security solutions and services are given in Section V. Section VI elaborates on the trust and privacy of NS. The lessons learned and envisaged future research directions are presented in Section VII. Finally, Section VIII concludes the paper. A list of important acronyms is given in TABLE I.

II. Network Slicing in a Nutshell

NS enables multiple independent E2E logical networks in the same physical network architecture. These logical networks, known as slices, are tailor-made to satisfy specific requirements demanded by a particular service, application, or particular vertical industries [48], [49]. In addition, multiple network slices can also be bundled together as a single product that caters to diverse and multiple requirements. For instance, an ultra-reliable slice may be required for assisted driving and telemetry while a slice with high bandwidth may be required for infotainment in a connected autonomous vehicle [50]. Network slices can be created in 5G and beyond mobile networks owing to technologies such as SDN, NFV, network automation, analytics, and orchestration. Different network characteristics including network speed, latency, reliability, security and data processing capabilities of each slice can be customized according to Service Level Agreement (SLA) in 5G networks [48]. Each network slice comprises of shared and/or dedicated network resources such as storage, bandwidth, and processing power. A network slice can not only span across many parts of the network like transport network, terminal, core network, and access network but also extend across several mobile operators [52]. Furthermore, the services offered by a network slice can be categorized into two logical components, namely, network connection service and network resources service, as briefed below [44]:

Network connection service: The functionalities offered at the connection level to the customers is described by the network connection service. The operator is expected to provide the following characteristics regarding to the connection service to the customers such as near real-time latency, reliable and stable download and upload speeds, guaranteed SLA, seamless network coverage across several networks and also across the country borders, management of connected devices, seamless mobility, energy efficiency, and data security.

Network resources service: Apart from providing resources for executing proprietary applications, and life-cycle services to the customer, the network should be able to provide more platform services such as big data analytics, asset/ ID management, platform security, dynamic charging of real-time interactions, cloud computing, edge computing, partner integration, and providing APIs for several control and management capabilities.

A. Architecture of Network Slicing

The general NS architecture comprises of three functional layers, namely, the service instance layer, network slice instance layer, and resource/infrastructure layer, as depicted in Fig. 2 [25]. The Network slice controller/orchestrator is responsible to coordinate the operations of each layer.

1) Service Instance Layer: This layer runs on top of the other layers and provides business and end-user services, which may be provided by a third party or the network provider. The business or end-user services are supported by the service instance layer (a run-time construct known as an "instance" is derived from configuration time or design time "blueprint" or a "template"). In the application layer, each service requested by different applications is represented as a service instance, that merges the network characteristics in the form of SLA requirements which should be satisfied by the creation of a suitable slice [53]. A service instance can represent either a service provided by the operator or a third party.

2) Network Slice Instance Layer: This layer runs in between the service instance layer and resource/infrastructure layer and is responsible for creating and managing network slices based on the requests from the application layer. A network slice blueprint is used by the network operator to

create the network slice instance. The network characteristics required by a service instance are provided by a network slice instance, that can be shared across network operator's service instances. The network slice instance can also share sub-network instances with other network slice instances. Network functions that can run on a logical/physical resource are formed from the sub-network instance, that is created by the sub-network blueprint.

3) Resource/Infrastructure Layer: The resource/infrastructure layer is responsible for providing and managing network resources (both physical and virtual) such as connectivity, computing, and storage. Based on the characteristics requested by the service, an E2E slice is created by the network functions present in the virtual network infrastructure. The network operations configure the network functions to manage the full life-cycle of the operations right from the creation of the network slice till the slice is de-allocated when the provided function is not required. The same network functions can be shared by multiple slices simultaneously for efficient usage of the resources, which may lead to increased complexity in the management of the operations. These network functions can run utilizing either be physical or virtual resources available in the network.

4) Network Slice Controller/Orchestrator: The network slice controller/orchestrator interfaces with each layer in the NS architecture to coherently manage and coordinate their diverse functionalities efficiently [32], [54]. This ensures the flexible and efficient creation of network slices that can be reconfigured during different phases of the NS life cycle. The major functionalities of the network slice controller are as follows:

- *E2E service management:* It maps several service instances according to the SLA requirements with corresponding network functions satisfying service constraints.
- *Virtual resources:* It is responsible for physical network resources' virtualization to ease operations for the management of resources that assign network functions.
- *Slice life-cycle management:* It is responsible for monitoring the performance of the network slice in all the layers of the architecture to reconfigure every slice for accommodating the modification of SLA requirements.

B. Life-Cycle of a Network Slice

The life cycle of a network slice comprises four phases. They are the preparation phase, commissioning phase, operation phase, and decommissioning phase. The phases of the network slice life-cycle are illustrated in depicted in Fig. 3.

Preparation Phase: The first phase in the life cycle of a network slice is the preparation phase. In this phase, the following tasks are performed:

- Creation and verification of network slices based on the requirements/needs of the customer
- Preparing the required network environment for facilitating the life cycle of the network slice
- Network slice capacity planning
- On-boarding of the network slices
- Evaluating the requirements of network slice

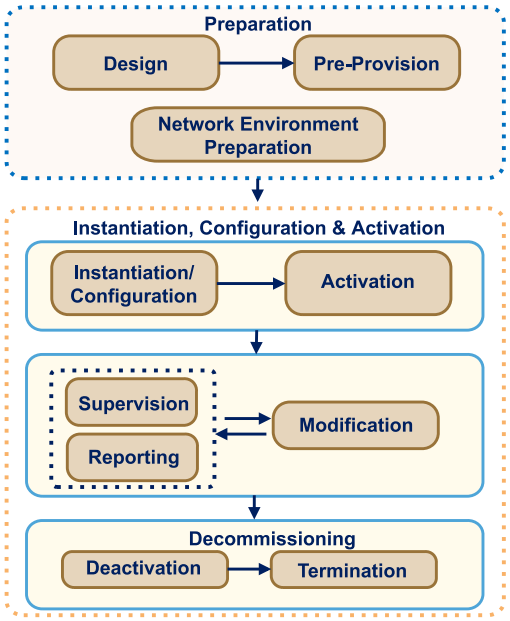

Fig. 3. Life Cycle of Network Slice.

- Identification and preparation of additional requirements for the network.

Commissioning Phase: After this phase, the network slice will be ready for operations. This phase is responsible for the following tasks:

- Network resources allocation
- Facilitating the requirements of the slice by executing the required configurations.

Operation Phase: The operation phase is responsible for the following tasks:

- Activation: Several processes such as provisioning databases, and traffic diversion to the slice activate the network slice.
- Supervision: Continuous supervision of the network slice has to be done.
- Monitoring of key performing indicators: The network slice has to be continuously monitored based on the key performing indicators.
- Modification: Several tasks such as reconfiguration, upgrading, updating the topology, scaling, association, and disassociation of the network slices are performed here.

Decommissioning Phase: The network slice will be terminated after this phase. Tasks performed by this phase are:

- Reclaiming the resources which are allocated dedicated to the network slice
- Reclaiming the configurations from the resources that are dependent/shared

However, it should be noted that these life cycles are required to be managed carefully, as their security and privacy vulnerabilities are yet to be explored. Not only, life cycle security, but many other aspects of NS including inter-slice security, intra-slice security, and SLA management needs careful attention to ensure that network security and user privacy are not compromised.

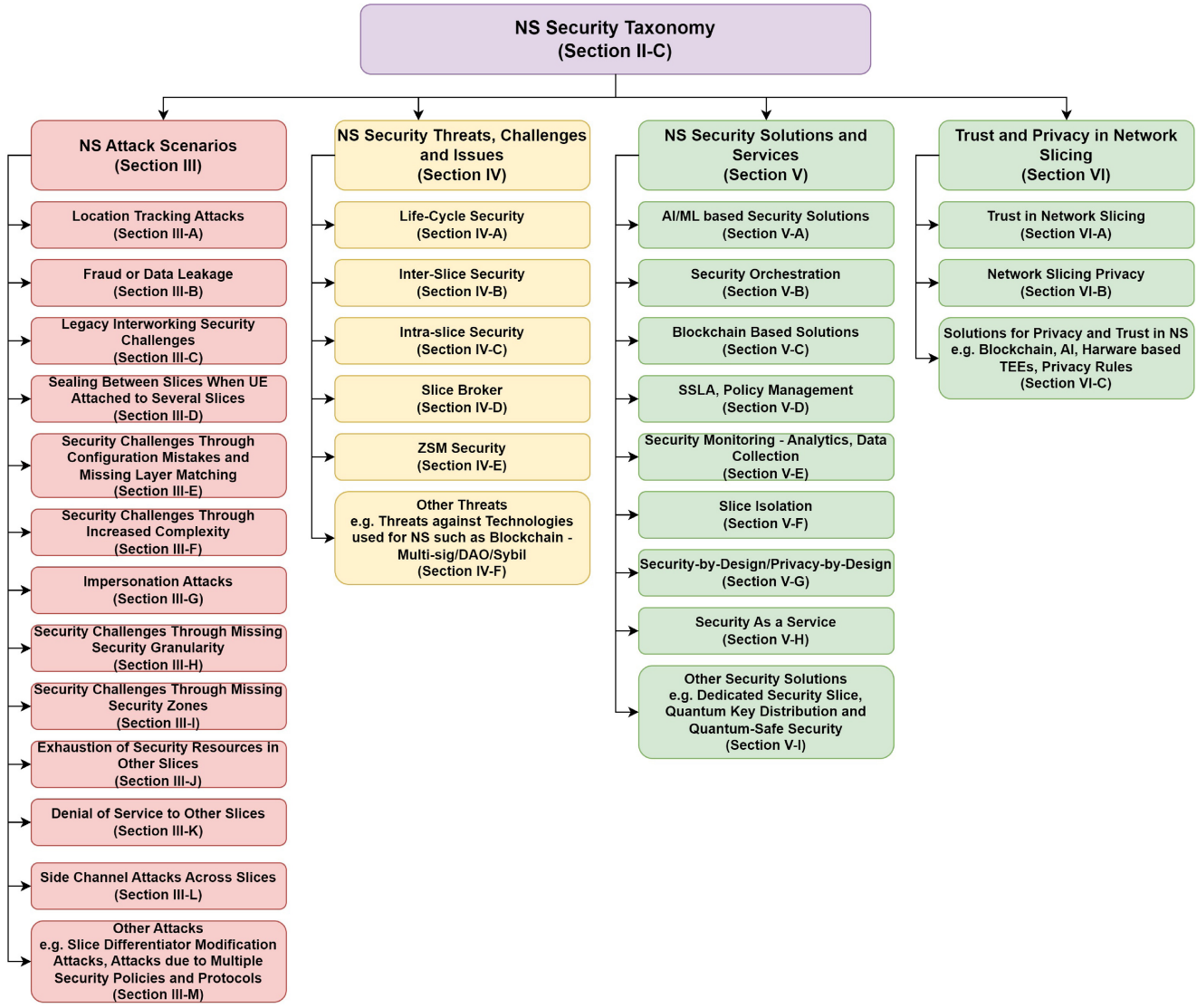

Fig. 4. Network Slicing Security Taxonomy.

C. NS Security Taxonomy

The number of attacks targeting mobile networks is on the rise with the growth of many digital applications and services delivered over mobile networks expanding across many sectors ranging from finance, health, education, and smart cities to e-governments [39]. For instance, the attack against the Australian mobile network operator Optus has compromised customer information resulting in many attacks including phishing attacks, identity theft, and Subscriber Identity Module (SIM) porting [55]. While expanding the capabilities of mobile networks, the introduction of NS to mobile networks will extend the threat landscape of mobile networks. In response, we formulate an NS security taxonomy, as illustrated in Fig. 4. The proposed taxonomy discusses NS Security in the areas of attacks, threats, challenges, issues, and security and privacy solutions.

1) NS Attack Scenarios: NS is envisaged to be a key technology in 5G and beyond networks. However, NS also opens new attack surfaces and opportunities. These attacks can range from location tracking attacks, and fraud or data leakage attacks, to side-channel attacks across slices. Key attack scenarios of NS systems are explored in Section III.

2) NS Security Threats, Challenges and Issues: Considering the various attack scenarios for NS, a new landscape of threats, challenges, and issues are realized. These include life-cycle security, intra-slice security, inter-slice security, slice broker security, and Zero-touch network and Service Management (ZSM) security. The security threats, challenges, and issues related to NS are discussed in Section IV.

3) NS Security Solutions: Various security solutions are proposed for resolving the security threats, challenges, and issues of NS. These solutions range from Artificial Intelligence based solutions, and security orchestration, to offering security as a service. Section V proposes security solutions and services for overcoming the security challenges inherent to NS-enabled 5G and beyond networks.

4) Trust and Privacy in Network Slicing: Ensuring trust and privacy in mobile networks is paramount. NS privacy and trust aspects are discussed in Section VI.

Therefore, following the structure of the proposed taxonomy, NS attack scenarios are discussed in Section III, NS security threats/challenges/issues are presented in Section IV, NS security solutions and services are elaborated in Section V, and NS trust and privacy are considered in Section VI.

III. Key Attacks Scenarios in Network Slicing System

Being an evolving concept, NS poses the risk of facing various attacks. The impact of these attacks is yet to be seen due to the limited number of 5G networks with NS. However, the impact of NS attacks will be significant as more and more mobile networks embrace NS in their 5G networks. This section explores several attack scenarios in NS.

A. Location Tracking Attacks

Location tracking attacks in NS can be performed by a misbehaving NF to track the location of a target user in another NF [56]. When a Network Function (NF) consumes a service from another NF, the NF that consumes the service requires an authorization ticket in order to use features including location tracking. A misbehaving NF may obtain an authorization ticket and send a request to the location tracking server using the identifier of a target user from a slice. This is possible as any correlation matching is not performed between the authorization ticket and the user identity. Hence, checking if the user identity belongs to the particular slice that raises the request to track the location is not performed. Thus, attackers can obtain the device location of the target.

In addition, hybrid network functions in 5G networks support several network slices and have no solid mapping between the application layer identities and transport layer identities [56]. This exposes NS-enabled 5G networks to another threat leading toward location tracking. Attackers are able to gain access to user locations through hybrid network resources.

Furthermore, user location data can also be exposed by a hacker who can compromise the edge network functions of an NS-enabled 5G network. This is through exploiting design flaws in NS standards in order to access 5G services provider's core networks resources and network slices.

The likelihood of these attacks may increase as more 5G networks deploy NS. However, it should be noted that these vulnerabilities are already listed under the Global System for Mobile Communications Association (GSMA) Coordinated Vulnerability Disclosure (CVD) program [57]. This would facilitate future research and development work to secure NS-enabled 5G networks against location-tracking attacks.

Summary: Location tracking attacks exploit vulnerabilities of NS-enabled networks to track the location of a target user. These attacks can be performed in several ways, including, exploiting misbehaving NFs, design flaws of hybrid NFs, and compromising network edge functions [56]. The impact of each of these attacks against NS is yet to be explored. However, these vulnerabilities are listed in the GSMA CVD program [57] to facilitate future research towards strengthening the security and privacy of NS-enabled 5G networks.

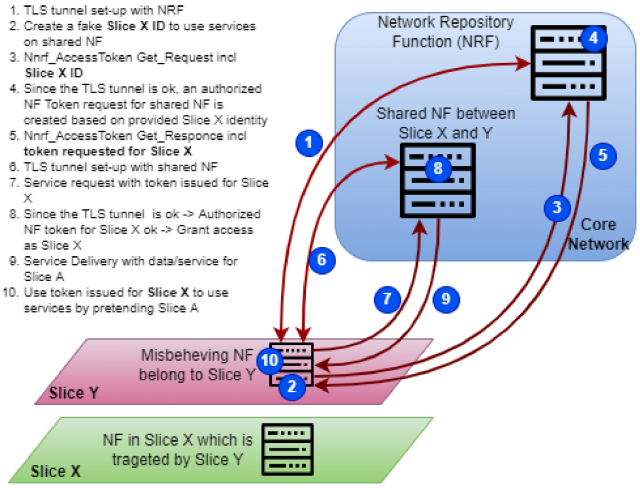

Fig. 5. Possible Fraud or Data Leakage Attack via Service Theft.

B. Potential for Fraud or Data Leakage

The fraud or data leakage attacks [58] are targeting the information or data from one slice to another. If these two slices serve two different verticals, services of a network function and related information of another vertical can be stolen by the fraudulent vertical. When the network functions are shared by multiple slices (or multiple verticals), it is possible to exploit such fraud or data leakage attacks if proper authentication mechanisms are not utilized [32].

Figure 5[1] illustrates one of the possible fraud or data leakage attack via service theft. When multiple slices utilize the shared NF, an authorization ticket is used by each NS to request the services from the particular NF. In this case, the fraudulent vertical slice (i.e., Slice Y) impersonates slice X and obtains the authorization ticket from the Network Repository Function (NRF). Currently, the complete details that should be included within the request are not well specified by 3GPP standards. Thus, everybody in the network can ask for any ticket without proposer security validation. Due to this, when NF in Slice Y request an authorization ticket, It could put Slice X's identity (e.g., instance ID, slice ID, IP address) and get the authorization ticket generated for Slice X. Using this, Slice X's authorization ticket, slice Y could do serious fraud and steal sensitive data of subscribers when they are processed within the shared NF.

During this type of attack, the fraudulent vertical can impersonate another vertical and use the services under the account of the victim vertical. The victim vertical might not be aware of such an attack. For instance, the victim vertical may have to pay for a service it did not use or order. Usually, the network function sharing is enabled between slices shared by 'trusted' vertical partners. Detecting these attacks is more challenging when they originate from the 'trusted' vertical partners.

The current 3GPP standard proposed to use authentication and communication security using TLS (Transport Layer Security) [59], [60]. However, TLS is insufficient to secure the slices against these attacks [61], [62]. Therefore, we should

[1]5G Network Slicing Vulnerability: Potential for Fraud or Data Leakage https://blog.adaptivemobile.com/5g-network-slicing-vulnerability-fraud-data-leakage.

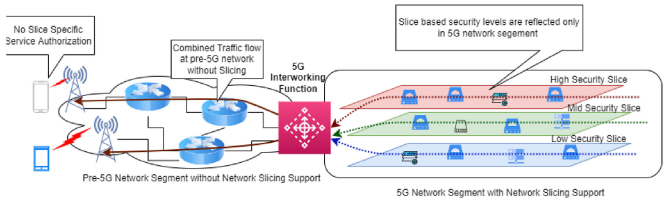

Fig. 6. Security Challenges in Network Slicing through Legacy Interworking.

find advanced security authentication mechanisms to mitigate these attacks. Moreover, simple trusting mechanisms are not enough to secure shared NF utilization in 5G network slicing systems. Advance trusting mechanism, such as trust and reputation models [63], computational trust [64], blockchain [65] or Zero-trust security [66] should be utilized to prevent these attacks.

Summary: Fraud or data leakage attacks target information or data from one slice to another [58]. This attack can be performed by exploiting shared NFs [32]. Furthermore, existing solutions for securing NS against such attacks, including TLS [59], [60], are not sufficient to secure NS. This requires future research work to explore advanced trusting mechanisms, such as trust and reputation models [63], computational trust [64], blockchain [65] or zero-trust security [66] towards mitigating fraud or data leakage attacks against NS.

C. Security Challenges Through Legacy Interworking

5G deployment and roll-outs have been happening worldwide for the last few years. However, the transition from pre-5G to 5G network is not happening as an overnight task [67]. It is a gradual process. The MNOs have already made a lot of investment to deploy pre-5G network infrastructure, and they are unwilling to abandon them to deploy pure 5G networks. Thus, it is very likely for many MNOs to have pre-5G network segments in their networks [68]. Thus, it is prudent to assume that they will continue to support many legacy pre-5G functions in their network [69], [70]. The network slicing concept was introduced with the advent of 5G networks. It was not implemented in pre-5G networks. Therefore, deploying network slicing-based services may require having a pre-5G network segment without slicing support. Such instances can also occur during roaming events when users roam between 5G and pre-5G networks [71]. It is understandable since not every MNO worldwide will move at the same speed to deploy 5G networks.

The deployment of network slicing in such mixed network architecture needs careful security considerations. Especially various security challenges can arise via legacy interworking. For instance, slice-specific service authorization is challenging to deploy when users are connected via 4G networks, and the 4G interworking function converts communication from that 5G slice to the 4G network. Moreover, The 5G interworking function will appear as the interface for the whole pre-5G legacy network segment. This prevents the deployment of slice-specific security services. Moreover, it is impossible to support slice isolation at the pre-5G network segments, which may lead to side-channel attacks. Figure 6 illustrates the security challenges for network slicing due to legacy interworking.

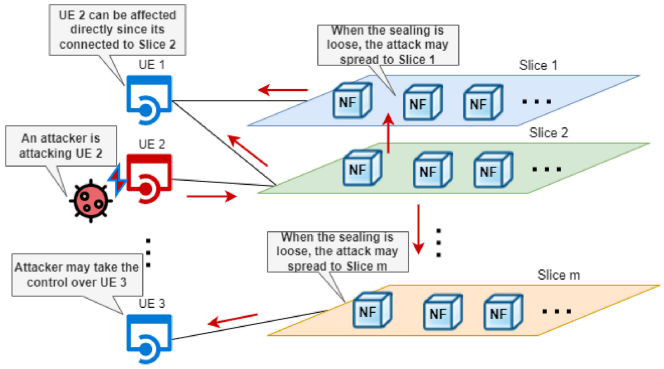

Fig. 7. Security Challenges of NS without Proper Sealing between Slices.

Summary: The transition from pre-5G to 5G networks happens gradually while MNOs remain keeping pre-5G network segments supporting pre-5G network functions [67], [68], [69], [70], [71]. Deploying NS in such networks gives rise to various security threats, due to reasons such as, the lack of slice-specific security features, slice isolation capabilities in pre-5G network segments, lack of support for virtualization and incompatibilities.

D. Sealing Between Slices When User Equipment (UE) Attached to Several Slices

When the UE is attached to several network slices, that particular UE may create an explicit linkage between the network slices while acting as a common access point to multiple slices at the same time. However, those slices may have different levels of sensitivity. When there is no clear separation among the slices, an information leakage may create serious security and privacy issues. For instance, the UE can publish the received sensitive data from one slice via another slice to which it has access. Although the UE has direct access to the RAN layer, when it is connected to multiple network slices, it has the possibility to access the respective network functions which are running in the different network slices of the core network [42]. Similarly, if one connected slice is attacked and the attacker can take control of the UE, it may impersonate the UE to impose an attack on the other network slice as well. This will proliferate the propagation of security attacks over multiple network slices. As illustrated in Figure 7, when the proper sealing is not implemented between the slices, the attacks may spread between the slices and the attacker can take control of UEs which are connected to those affected slices.

Summary: UE attached to several network slices links network slices while acting as a common access point to multiple slices with various levels of sensitivity. This may lead to attackers targeting NFs in other slices. Furthermore, an attack for one NS may result in controlling the UE irrespective of the security measures in other slices. This demands security solutions providing proper sealing between network slices.

E. Security Challenges Through Configuration Mistakes and Missing Layer Matching

It is important to identify the efficient resource configuration as well as the security configuration strategies of the

network slices [72]. On one hand, the networking resources and security policies can be assigned to a network slice in a static or dynamic manner. On the other hand, it is desirable to consider the trade-off between the selection of strategies for slice configuration with respect to the cost that incurs. When the security policies and security service level agreements are defined at the initial phase of slice configuration, it is necessary to identify the security requirements expected from that particular network slice. Based on the resource allocation and security configuration of that network slice, the attack resistivity will be defined. When there are configuration mistakes at the initialization phase of the network slice, those may impose serious security threats during the operational phase, especially in terms of attack resistance.

Moreover, network slice configuration is getting more complicated for layer matching when the slice requirements (i.e., both security and resource) are complex [73]. For instance, when a malicious network function in one network slice tries to establish connectivity to a service provider's NRF, it may access the central storage of all the network functions in the provider network. The malicious function may access another network slice that is running with the same network. Since both network slices share the same network functions and the NRF is aware of that, this will be a valid request and a token can be generated for the target network slice. Thereby the rogue slice will be able to access the information in the other slice.

Summary: Configuring NS can be performed considering several factors, including, resource utilization, security strategies, and cost [72]. However, any mistake in slice configurations or any missing layer matching, especially when the networks are complex, imposes serious security threats in terms of resistance to attacks [73]. Attackers can exploit such vulnerabilities in NS-enabled 5G networks.

F. Security Challenges Through Increased Complexity

The more complicated mobile networks become with more features in order to facilitate advanced applications and services, the higher the possibility of a mistake being made in designing, setting up, and configuring a mobile network. The network complexity with 4G has increased significantly with the dawn of 5G. For instance, inter-mobile network operator commands/messages have increased by 4.7 times and inter-mobile network operator information elements/attributes have increased by 3.4 times from 4G to 5G [74]. Each of these commands and elements needs to be inspected to ensure the security of the networks. The host MNO, who is responsible for slice management, needs to protect network resources as well as NS customers to prevent any attacks. This will be a significant challenge as more and more 5G networks deploy NS in their networks. Hence, mobile network service providers will have to carefully design, deploy and configure complex networks without any mistakes that may arise due to the complexity of NS-enabled 5G networks. Furthermore, NS will result in user activities leaving the scope of the mobile network operator and malicious slices entering the network. Therefore, mobile network operators should take sufficient measures to ensure security amidst high complexities in NS-enabled 5G networks.

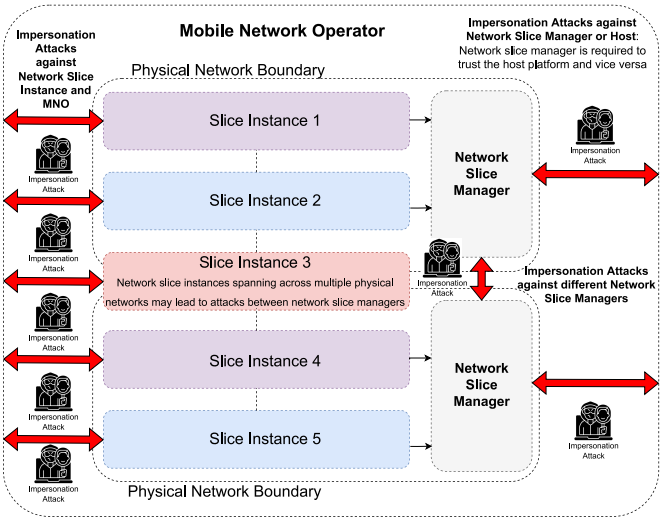

Fig. 8. Security Challenges of NS through Impersonation Attacks.

Summary: 5G networks have become significantly more complex than pre-5G networks [74], resulting in increasing the challenge of properly setting up, deploying, and configuring an NS-enabled network, which can leave opportunities for attackers to exploit.

G. Impersonation Attacks

Impersonation attacks, where the attacker appears as a trusted party, can also target an NS-enabled network [15]. This can happen is several methods, as indicated in Fig. 8.

One such method is impersonation attacks against a network slice manager or host. The network slice manager is required to trust the host platform to run the network slice. On the other hand, the host platform is required to trust the network slice manager. This may lead to impersonation attacks on the MNO, which exposes their network and services. Therefore, network slice managers and host platforms need to support mutual authentication. The network slice managers need to authenticate host platforms in networks, in which the network slices are to be deployed. The host platforms are also required to authenticate the network slice managers prior to deploying network slices.

Furthermore, impersonation attacks can happen against a network slice instance within an MNO. For instance, the authorized network slice instance may be dropped and replaced by a new instance. This can happen due to legitimate causes, such as element failure or restoration of lost functionality with a new instance. However, it is possible for a new instance to be created due to malicious purposes, which is difficult to be identified. This may affect all the services supported by the network slice instance. Therefore, all the functions within a network slice instance are required to be authenticated in order to verify their integrity.

Another way of performing impersonation attacks against network slicing is attacks against different network slice managers within an MNO. In the case of network slice instances

spanning multiple physical networks, multiple network slice managers are required to be deployed. This needs the network slice managers to trust other network slice managers to deploy a portion of the network slice instance. However, there might be issues in trusting other network slice managers, as they might be imposters. Through the network slice controlled, an imposter network slice manager may cause attacks that would impact all the services provided by that manager. This requires all network slice managers operating within an MNO to mutually authenticate each other.

Summary: Impersonation attacks are caused when the attacker appears as a trusted party [15]. This type of attack can happen to NS enabled network in several ways, including, against a network slice manager or host, against a network slice instance within an MNO, and against different network slice managers within an MNO, as illustrated in Fig. 8.

H. Security Challenges Through Missing Security Granularity

The B5G/6G service-based architecture, along with NS features, possesses a lot of flexibility and diversity in catering to the enabling requirements of various applications. However, it is quite challenging to configure it correctly on a granular level [74], [75]. For example, as discussed in subsequent subsections, slice identities play a crucial role at the slice management center by ensuring that the network-level resources and functions of orchestrated service are allocated to the right user (device or equipment) and corresponding network slices. Similarly, the authorization framework in the SBA architecture at the service and slice level is also crucial. However, at the granular level, the exchange of critical informational elements (e.g., device identity, cellID) to/from the selected network slices is crucial from a security perspective.

During the discussion in Sections III-B and III-E, we conferred on how the NRF of the slice manager issues access tokens and how to trust in the slice identity is related to the tokens. For example, Fig. 5 illustrates the TLS tunnel setup with NRF via NS service theft which creates the possible scenario of possible fraud (or data theft). Nevertheless, authorization granularity presents another security challenge. An NRF token could be issued for another slice if the rogue slice is successful in tricking it. Despite the fact that the authorization token is bound to an orchestrated network service, associated network function, and a corresponding slice identity, the actual request to the deployed service may contain a wide range of information.

As an example, Fig. 9 illustrates an API description of how the shared access and mobile management functions (AMF) allow the location information of a UE to be requested. The preliminary step-1 would involve setting up a TLS connection with the NRF by a rogue network function belonging to Slice 2 (i.e., NS-2). A check was not performed throughout the entire process to ensure that the UE identity in NS-1 was included in the service request sent from the rogue network function to the shared network function (NF). Hence, for a rogue slice to refrain from requesting information belonging to another slice on the granular slice level at service management,

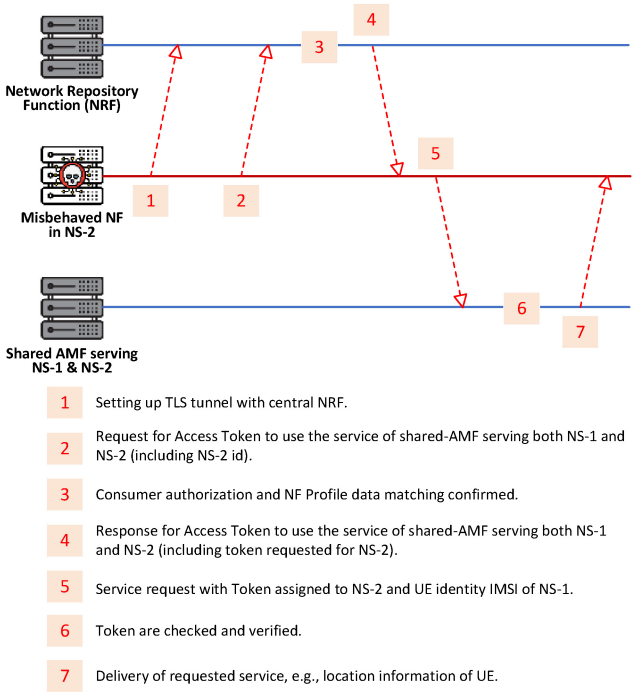

Fig. 9. Example Illustration of Information Leakage Risks between the Dedicated and Sharing NFs through NS Information Elements.

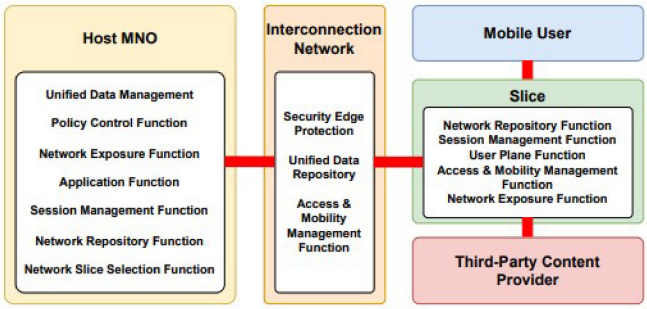

Fig. 10. Security Challenges in NS through Single Security Zone in Network Core.

it is important to verify the identity of each information element and slice identities before assigning access tokens and allocating resources.

Summary: Configuring complex 5G and beyond networks at the granular level is a challenge and requires the exchange of critical information element [74], [75]. This information may be acquired by rouge slices, which demands strict verification of slice identity before sharing information.

I. Security Challenges Through Missing Security Zones

Conventionally, the core network of the Mobile Network Operator (MNO) is considered a single trust zone. However, this approach in legacy networks is not suitable for NS-enabled 5G networks. This is due to the 5G service-based architecture offering access to network functions via APIs to third parties with different trust levels [76].

For instance, in order to provide localized streaming services to mobile users, a Mobile Virtual Network Operator (MVNO) slice would require the location of the users. This would require the MVNO slice network function to access

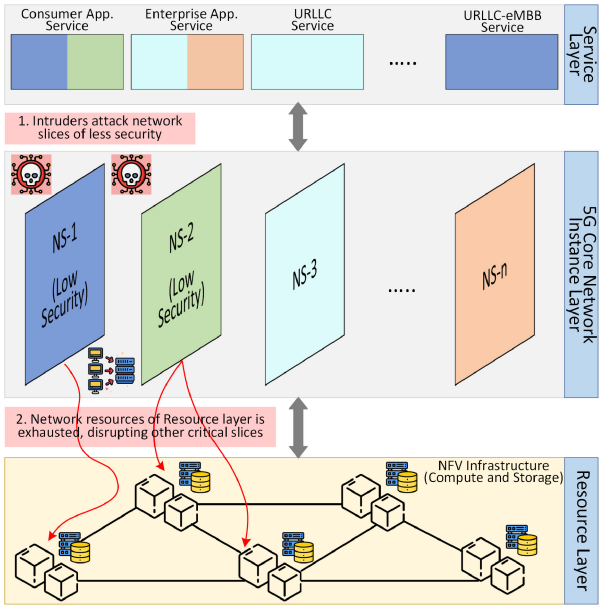

Fig. 11. Exhaustion/Depletion of Security Resources in Other Slices.

the access and mobility management function and unified data management of the core network of the MNO, as illustrated in Fig. 10. Thus, third-party content developers and application developers, who are in the same trust zone, can gain access to network functions through the MVNO slice. Therefore, the mobile network is required to operate at different trust zones in order to mitigate the risk of third parties controlling network functions. Another example is security issues related to inter-slice communication. A vehicular network slice may interact with both an entertainment network slice with large bandwidth and a Vehicle to Everything (V2X) network slice with low latency and ultra-high reliability. These two slices should also be considered as different security zones and the inter-slice communication should be filtered, authenticated, and authorized.

Therefore, the MNO core can be attacked through NS with the conventional model of considering the core network as a single trust zone. Therefore, the network architecture should facilitate the operation in different trust zones in order to facilitate secure network slicing in 5G and beyond networks [29].

Summary: Traditional network architecture considers the entire core network of an MNO as a single trust zone. However, 5G and beyond network architecture allows third parties access to different NFs., which can compromise the security of the network [76]. This demands a network architecture with different trust zones for 5G and beyond networks [29].

J. Exhaustion of Security Resources in Other Slices

The exhaustion in network slices is a phenomenon where the attacker attacks a slice with lower security levels after depleting the network function resources that are common to multiple slices (c.f. Fig. 11). For instance, the attacker would attack consumer slices rather than going for enterprise or industrial IoT slices as they have an enhanced level of security. However, the attacker would attack consumer slices after depleting resources such as processing power, memory, and hardware resources.

1) Impact of the Exhaustion Attacks and Solutions: A few studies have highlighted the resource exhaustion issue and its impact on the network slices and proposed recommendations to cope it, accordingly. Some of them are;

1) *Deep Neural Networks Usage.* Kuadey et al. [77] highlighted the use of Distributed Denial of Service (DDoS) attacks as a potential cause for depleting resources in network slices. The study proposed the use of deep learning network that uses long short-term memory (LSTM) networks for detecting DDoS attacks from network traffic at the user equipment end. The study suggests that by doing so, the exhaustion of resources in network slices can be prevented. Mathew [30] highlighted several security concerns with respect to network slices. In the study, the author highlighted resource exhaustion issues in network slices concerning 5G networks and suggested that the attack can be initiated using DDoS and impersonation attacks, respectively. Similarly, Thantharate et al. [78] also proposed the use of a deep learning framework for defense against DDoS attacks in 5G network slices. The study suggests that the development of a neural network-based method for the detection of network slice exhaustion attacks is in the works and the use of ring-fenced resources is a potential solution to cope with the exhaustion attack, accordingly. Furthermore, the study suggested that the security protocol resources should be preallocated to each network slice so that an individual slice can operate irrespective of other slices with depleted resources.
2) *Integrating Network Slice Isolation.* Kotulski et al. [79] focused on the network slice isolation in 5G networks and considered it as a potential solution for several associated attacks. In this study, the authors first highlight the use of DDoS attacks for exhausting resources. They then suggest the use of ring-fencing to cope with the aforementioned problem so that a network slice cannot exhaust other slice resources. Furthermore, the authors highlighted that the exhaustion problem is mostly related to the radio access network (RAN) part rather than the CN part of the 5G network, therefore, they suggested optimizing the RAN part for the prevention of resource exhaustion, accordingly.
3) *Incorporating Scale-out Operations.* Addad et al. [80] discussed the issue of network slice mobility in next-generation networks. The study proposed the use of scale-out operation suggesting that some services or users must be migrated to other centralized clouds or edges in order to reduce the impact of exhaustion attack while trading off with quality of service or quality of experience, accordingly.

Summary: This type of attack concerns the security implications for network slicing through the exhaustion of resources. Possible solutions are the use of deep neural networks [30], [78] to detect DDoS attacks that cause resource exhaustion, integrating NS isolation [79] and using ring-fencing to prevent a network slice exhausting other slice resources, and incorporating scale-out operations [80] to

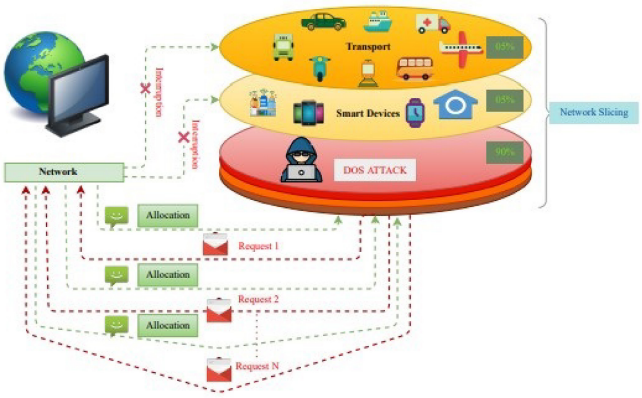

Fig. 12. Denial of Service to Other Slices.

minimize the impact of exhaustion attacks. However, further research is required to identify the impact of each of these solutions and seek the possibility of implementing these solutions in a complementary fashion toward strengthening NS security.

K. Denial of Service to Other Slices

In NS, several virtual networks are overlayed over a shared network domain. In some cases, the network resources may be shared across multiple slices. An intruder or an attacker can exhaust resources in one slice in the shared environment, thereby draining the resources that are common to multiple slices as depicted in Fig. 12. This phenomenon of exhausting the resources in one slice will cause DoS in other slices that have shared resources with that slice [77]. To prevent DoS attacks on NS, machine learning techniques and blockchain can be deployed. Machine learning-based models can be used to identify malicious users or attackers and hence can be denied requests to access a slice. Similarly, blockchain can ensure only genuine users enter into the network [81].

Kuadey et al. proposed a lost short-term memory-based deep learning framework, named as DeepSecure, to detect whether a user equipment (UE) traffic is normal or distributed DoS attack. If the UE request is legitimate, an appropriate slice is allocated to it [77]. In another interesting work, Hewa et al. have proposed a blockchain-based solution, named Security Service Blockchain (SSB) to prevent DoS attacks on network slice brokers. In this work every request SSB validates every request and hence controls the access of mobile network operators as well as tenants of IoT to the slice broker [82].

Summary: This type of attack concerns on attackers exhausting resources in one slice to the denial of service of one slice to drain resources that are common to multiple slices. This will cause DoS slices that have shared resources with the compromised slice [77]. Malicious users or attackers can be detected through machine learning and deep learning-based models and blockchain-based models can be developed to ensure that only genuine users enter into the network [77], [82].

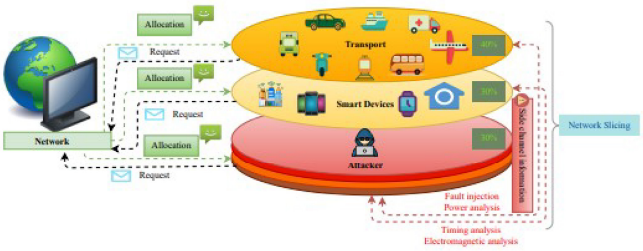

Fig. 13. Side Channel Attacks Across Slices.

L. Side Channel Attacks Across Slices

In a side-channel attack, the attackers try to extract the secrets of a system by analyzing or measuring several physical parameters such as electromagnetic emission, execution time, supply current, etc [83], [84]. By observing and analyzing these parameters, the attackers can influence the cache's content or may induct faults in the platform. These attacks can pose a serious threat and are proven to break cryptographic operations and thereby extract the secret key [85]. For instance, assume that two slices X and Y share some hardware. If an attacker can influence or observe the working of code in slice X, the attacker can influence the working of the code in slice Y/ extract the data about the code running in slice Y. These kinds of attacks may result in the attacker getting hold of secrets/cryptographic keys of slice Y as depicted in Fig. 13 [86]. One possible solution to prevent the side channel attacks in network slices is about the strong isolation of slices, i.e., even if an attacker can influence/observe how a code runs in one slice, he should not be able to extract the information on how the other slices run the code in the same hardware. Another possible solution to evade side-channel attacks is to prevent hosting the applications on slices with similar hardware with various levels of sensitivity/vulnerabilities that can be influenced by an attacker.

Summary: Side channel attacks attempt to extract information by analyzing physical parameters. This has the capability to break cryptographic operations by extracting secret keys [85], [86]. Possible solutions are strong slice isolation and avoiding the hosting of applications on slices with similar hardware.

M. Other Attacks

Table III provides an overview of the attack scenarios discussed from Section III-A to Section III-L. However, attacks for NS are not limited to the ones presented in Table III. For instance, multiple security protocols and policies across different network slices may require different security requirements [74], [75]. In addition, some network slices may bank on virtualized NFs while some might not be available as virtualized NFs. However, the security should be maintained across various deployment modes. Similarly, security challenges posed through vulnerabilities, such as attacks by modifying the slice differentiator, may allow attackers to target NS-enabled 5G and beyond networks.

TABLE III
NETWORK SLICING ATTACK SCENARIOS

NS Attack Scenario	Uniqueness to NS	Impact of the Attack	Mitigation Strategies
Location Tracking Attacks [56]	NS makes networks more vulnerable	Divulging location information of users	Correlation matching between NFs, solid mapping between the application layer and transport layer identities in hybrid NFs, security/privacy by design [56]
Fraud or Data Leakage [58]	NS makes networks more vulnerable	Leaking data to unintended parties	Better slice isolation [32], trust and reputation models [63], computational trust [64], blockchain [65], zero-trust security [66]
Legacy Interworking Security Challenges [68]	NS makes networks more vulnerable	Various security threats due to lack of slice-specific security functions in pre-5G networks	Moving to 5G and B5G network structures supporting slice-specific security functions [69], [70]
Sealing Between Slices When UE Attached to Several Slices [42]	Attack unique to NS	Access NFs of other slices, compromised slices can control UE	Implement proper sealing between slices [42]
Security Challenges through Configuration Mistakes and Missing Layer Matching [72]	Attack unique to NS	Attackers exploiting vulnerabilities in NS to attack 5G networks	Careful configuration of NS considering security, resource utilization and cost [73]
Security Challenges through Increased Complexity [74]	Attack unique to NS	Challenges leave opportunities for attackers to exploit 5G networks	Properly set up and deploy 5G networks [74]
Impersonation Attacks [15]	Attack unique to NS	Divulge confidential data considering as a trusted party	Authenticate functions within slice instances, mutual authentication among slice managers [15]
Security Challenges Through Missing Security Granularity [74], [75]	NS makes networks more vulnerable	Leak critical information at the granular level	Strict slight identity verification [74], [75]
Security Challenges Through Missing Security Zones [76]	NS makes networks more vulnerable	Networks can be attacked if the whole core network is operated as a single trust zone	Filter, authenticate, and authorize inter-slice communication, implement different security zones [29]
Exhaustion of Security Resources in Other Slices [77]	Attack unique to NS	Compromise the security of slices by attacking lower security slices and depleting common resources	Deep neural networks to detect DDoS attacks [30], [78], slice isolation [79], ring-fencing to prevent exhausting slice resources, scale-out operations to minimize impact [80]
Denial of Service to Other Slices [77]	Attack unique to NS	Denial of service of one slice to draining resources common to multiple slices	Machine learning-based techniques for attack detection, blockchain for user access control [77], [82]
Side Channel Attacks Across Slices [85], [86]	Attack unique to NS	Attackers extract information	Strong slice isolation, avoid hosting applications on slices with similar hardware [86]

IV. SECURITY THREATS, CHALLENGES AND ISSUES

In the preceding sections, its is established that network slicing allows different 5G services to share network resources from the same resource layer infrastructure to satisfy their specific service requirements, e.g., vehicular communication, e-health, video streaming, voice communication and so forth [41], [87]. Using NS, the differentiation of 5G services to various enabling vertical applications includes the performance enhancements such as network availability, reliability, error rate, throughput and latency, and network functionality comprising of control, security and mobility [79], [88]. Although NS has numerous advantages, it is also vulnerable to threats and probable points of attack, as illustrated in Fig. 14. Furthermore, potential threats/attacks in different components of NS are tabulated in Table IV. In Table IV, we classified and described the various attack types in NS systems according to the common key attacking scenarios within the 5G architecture, which are discussed in Section III. Moreover, the likelihood of various threats classes documented and observed in the literature studies related to the 5G NS system are also grouped according to different security concerns, and they are 1) life-cycle security, 2) intra-slice security, 3) inter-slice security, 4) slice broker security, and 5) ZSM security.

The rest of this section elaborates the above critical security concerns associated within the 5G NS system.

A. Life-Cycle (LC) Security

1) Introduction: The NS lifecycle (LC) management starts with the instantiation phase of a slice which comprises slice/catalog templates based on slice requirements. The slice creation phase starts after the slice policy is defined so that a request to the slice orchestrator (or MANO) could be forwarded for creating the slice and reserving the resources. The slice components are then instantiated followed by the activation of the slice for its usage and availability. The network slice monitors the demand in the activation phase while providing feedback to update the service demands in the monitoring phase. The slice is then deactivated, once it reaches its lifespan, hence the deactivation phase. Hence, considering the dynamic characteristics of a network slice, its life cycle needs to be managed.

The steps in network life-cycle management include creation, activation, update, and deletion, as illustrated in Fig. 14 needs to be organized by the network slice controller/orchestrator. There are various techniques proposed for orchestrating network slices in order to manage its life

TABLE IV
POTENTIAL THREATS/ATTACKS IN DIFFERENT COMPONENTS OF NS

References	Attacks Class & Scenario Types	Attack Class Description	LC Security	Intra-Slice	Inter-Slice	Slice Broker	ZSM Security
[78], [88], [91]	NS-enabled Malware Injections (Sec. III-J))	An active slice is used to inject malicious code or transfer executable content.	L	M	M	L	H
[4], [29], [88]	Leveraging Fake Slices (Sec.III-B & III-D)	Information is stolen or manipulated by an adversary hiding behind fake slices.	L	H	H	L	M
[29], [92], [93]	Deactivating Sensitive NS (Sec.III-B)	Attempts are made by the adversary to disable slices that contain sensitive information.	L	H	H	L	M
[94], [95]	Network Sub-slice attack (Sec.III-I & III-J)	The weakest sub-slice is attacked to compromise all inter-connected slices.	L	0 L	L	L	M
[4], [96]	Compromising Network Slice MANO (Sec.III-C)	Control-plane functionality is accessed by an adversary attacking the network functions managing network slices.	H	M	M	H	L
[88], [97], [98]	Connected NS Data Leakages (Sec. III-B)	During transmission between a secured slice and a less secure slice, an adversary attempts to access or tamper with the data.	H	L	H	L	M
[29], [99], [100]	Disrupting NS Service Interface Communication (Sec. III-L & III-E)	A service attack occurs when it is communicating with a slice.	H	H	L	M	M
[101], [102]	Attacks on Third Party NS (Sec.III-G)	The shared parameters of a slice occupied by a third party can be changed by accessing it from another slice.	H	L	H	M	M
[88], [103]–[105]	Associated NS API Attacks (Sec.III-E)	It gives intruder to access to slice activation, configuration, and installation processes.	H	M	H	M	L
[44], [104], [105]	NS Identity Theft Vectors (Sec.III-A)	Sessions, authorizations, and authentication are exploited in identity attacks.	H	M	H	L	L
[104]–[106]	Attacks on Intermediate NS-based Functions (Sec.III-F & III-D)	This relates to the interception and tampering of information during communication between network slices.	H	M	H	L	L
[29], [105], [107]	NS Service DoS Attacks (Sec. III-J & III-K)	It involves using multiple requests simultaneously to overload the slices and disrupt the services.	L	L	L	H	L

L Lower Likelihood Threats M Medium Likelihood Threats H High Likelihood Threats

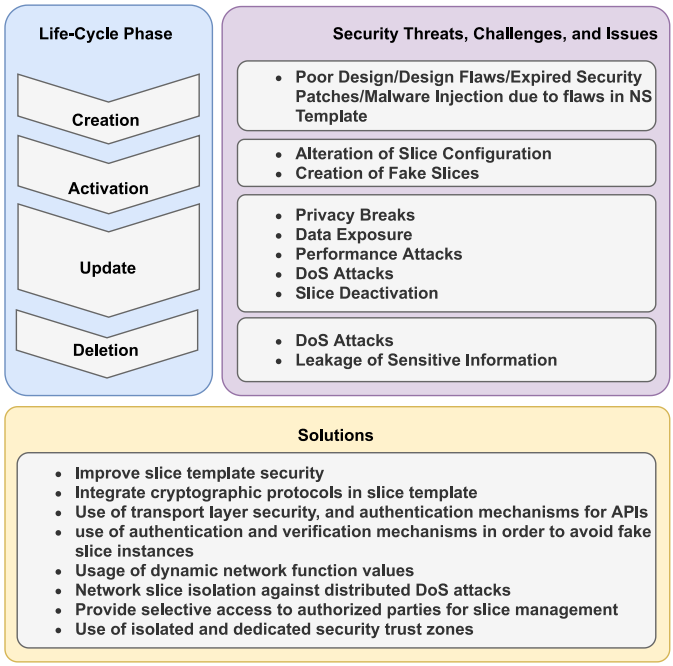

Fig. 14. NS Life-Cycle Phases, Threats and Possible Solutions.

cycle, however, the security vulnerabilities and threats while managing the life cycle are yet to be explored.

2) Security Threats, Challenges and Issues: There is security associated with each phase of the network slice lifecycle in 5G service architecture. As the 5G network slice is being prepared, it is vulnerable to malware injection, data leakage, content exposure, and similar threats (Table IV). In this way, unencrypted channels can be breached, and user information can be leaked from the database, resulting in the loss of authenticity, integrity, and confidentiality [87], [89]. At the activation phase, fake slices can be created or slices can be reconfigured during the slice activation at edge 5G gNBs (gNodeB). An example of such a point of attack can be an application program interface (API), which if compromised, would allow the hacker to interfere in slice activation, configuration, and even installation, process [87]. At the runtime phase, the target of attacks includes centralized control elements, control channels, overall cloud-edge system, hypervisors, and 5G MANO controllers.

A wide variety of attacks can affect the update phase including but not limited to privacy breaks, data exposure, performance attacks, and denial of service (DoS) attacks. These attacks can also affect the runtime process by making unauthorized changes and add new threats such as slice deactivation, respectively. API is also the central point of the attacks associated with the update phase [106]. At the deactivation phase, most of the time, the slice at this stage is under attack due to improper usage of network functions and resources, and improper handling for slice deactivation. The attacks at this stage can target centralized core elements, cloud storage, and information databases. Furthermore, it may lead to further DoS attacks and at worse, leakage of sensitive information [87].

3) Related Work: Ting et al. provides a discussion on the complete 5G architecture in [107]. This work explores various scenarios of 5G while also discussing potential security issues.

The security issues are discussed in the context of 5G architectural components, including concerns associated with the network slice life-cycle. The study also focuses on potential solutions for slice template security. The report from 3GPP [108] also highlights the security issues related to the network slice life-cycle and suggests integrating cryptographic protocols at the slice template's storage and transmission phase for providing better authenticity, integrity, and confidentiality. The study also suggests the use of good practices such as transport layer security, and authentication mechanisms for APIs. Khan et al. [4] provided comprehensive details regarding the 5G security issues related to slice life-cycle management. The study also suggests the use of authentication and verification mechanisms in order to avoid fake slice instances. Furthermore, the usage of dynamic network function values is suggested to mitigate run-time security issues by activating on-demand security methods. The work proposed in [105] highlights the security concerns in the update phase and proposes a mathematical model for network slice isolation that can handle the distributed DoS attacks in a proactive manner. Cao et al. [109] provided yet another in-depth review of 5G architecture with an emphasis on security features, and its solutions. They suggested selecting and providing access to authorized parties for deletion, modification, and creation of slice instances in order to be safe from attacks. Schinianakis et al. proposed the use of isolated and dedicated security trust zones during the NS life-cycle management in order to prevent unknown attacks and the creation and modification of network slices [110].

4) Countermeasures: Existing works propose several measures to provide better confidentiality and integrity of network slices concerning slice life-cycle. During the preparation phase, it is recommended to use encryption and decryption techniques for adding real-time security and perform analysis of the slice templates to avoid attacks. At the activation phase, it is recommended to secure APIs by providing accessibility and operational rights to the authorized people and also utilizing O-Auth and TLS protocols for authorization and authentication purposes. At the run-time phase, it is necessary to maintain the integrity and authentication of network slices to cope with fake requests. Furthermore, slice isolation is recommended to prevent DDoS and DoS attacks, whereas secure 5G modeling is performed to deal with malicious requests and unauthorized access. The system can also utilize an on-demand security mechanism by using dynamic network function virtualization, respectively. At the deactivation phase, it is recommended to deallocate the network functions and resources for the network slices that are not in use, properly, in order to avoid attacks. Furthermore, it is also recommended to delete sensitive information that is not required anymore.

B. Inter-Slice Security

1) Introduction: Using different network slices in an interlaced manner, inter-slice communication improves communication efficiency and effectiveness. Similarly, due to the varying characteristics of this type of communication, such as network resources, configurations, and requirements, their security management can be quite challenging. Hence, inter-slice communication security affects 5G customer devices, service-to-service communication, intra-slices and sub-slices communication, network management systems, and resource infrastructure, as illustrated in Fig. 15.

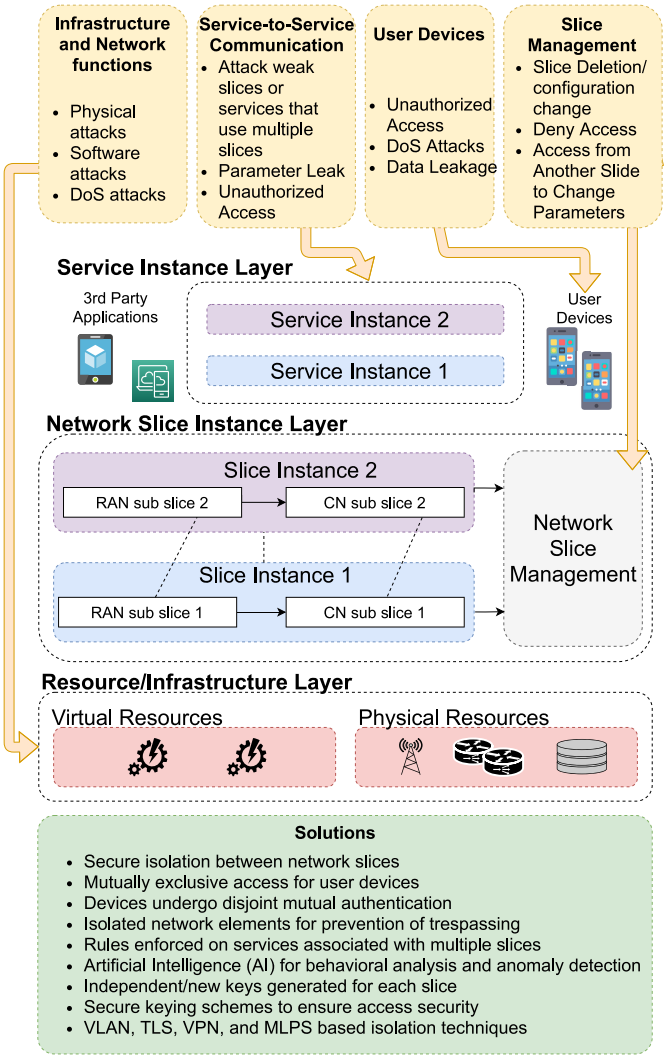

Fig. 15. Inter-Slice Security Threats and Possible Solutions.

2) Security Threats, Challenges and Issues: The major security threat for inter-slice communication comes from 5G user equipment that is authorized to access network slices. Some of them are highlighted in Table IV. The threat occurs when the same device tries to simultaneously access another network slice in an unauthorized way. This threat might lead to successful DoS attacks by excessively overwhelming shared resources, leading to performance degradation. This can also open up other threats as overwhelming network resources will resist conventional security protocols [29]. The risk of sensitive data leakage is also associated with such threats due to the transition of information from a secured slice to a less secured one. The threat level also increases in cases when the access technologies are not homogeneous [87]. Another point of attack, which may not be severe but still able to degrade the performance, is service-to-service communication.

The services can be stacked on top of each other or can be used in parallel. In both cases, a single service may simultaneously use multiple slices. The adversary might attack the services that use multiple slices at a time to damage the quality of service [111]. Furthermore, if the slices are able to communicate amongst themselves, an adversary may target a less secure slice (radio access network sub-slice) to attack more secure slices. This type of attack may lead to exposing sensitive data between multiple slices, leakage of parameters, and providing unauthorized access to network slices and other resources [110]. Furthermore, management systems that deal with third-party applications or resources can also be considered potential points of attack. This is due to a slice occupied by a one-third party that can try to access the slide from another one to change shared parameters [100]. Another potential point of attack is the resource layer which comprises of software execution for the given infrastructure. The adversary can use this point of attack to tamper with code to cause changes in all the slices that share the same execution code [100].

3) Related Work: The 3GPP standards suggest that secure isolation between network slices can help mitigate resource consumption, authenticity, integrity, confidentiality, and access control [87]. Furthermore, the standards also suggest mutually exclusive access for customer devices having simultaneous access to multiple channels. Khan et al. [4] conducted an in-depth review of security concerns and suggested that the 5G devices should undergo disjoint mutual authentication in order to access multiple network slices, simultaneously. The European Union Agency for Cybersecurity (ENISA) submitted a report that suggests the use of isolated network elements for the prevention of trespassing between services associated with a particular slice [111]. Furthermore, they also suggest that certain rules must be enforced on the service usage that is associated with multiple slices. Schinianakis et al. proposes the use of Artificial Intelligence (AI) techniques for behavioral analysis and anomaly detection to design the defense mechanisms for attacks associated with the services [110]. The report from Next Generation Mobile Network (NGMN) alliance recommends that independent and new keys should be generated for each slice in order to improve the authentication mechanisms and to secure the communication amongst multiple slices [100]. In addition, Porambage et al. discusses attacks concerning third-party applications for network slice management and suggests using secure keying schemes to ensure access security [99]. Furthermore, Kotulski et al. explores the use of isolated slices and security challenges associated with the creation of such slices [79]. Their study suggests using Virtual LAN (VLAN), TLS, VPN, and MLPS-based isolation techniques to strengthen inter-slice security.

4) Countermeasures: Existing studies concerning inter-slices have focused on the use of secure keying schemes, authentication, and isolated network elements for improving security. Some studies also suggest the use of AI for detecting anomalies in slice behavior. However, with the evolving attacks, security strategies are required to improve. One of the effective ways is to isolate the slices and use minimal communication between slices to stop the propagation of attacks. Also, encryption techniques that do not transmit public/private keys should be opted for slice security. There should be unique and independent access control, authorization, and authentication mechanisms for each slice. Furthermore, the access to make changes in slice configuration should not be given to third-party applications.

C. Intra-Slice Security

1) Introduction: The main difference between inter-slice communication and intra-slice communication is that inter-slice communication uses shared resources at the control layer, whereas intra-slice communication uses dedicated resources. Within intra-slice communication, each solution, component, and function is designed to solve and address specific issues related to specific applications such as e-health, and IoT. Because intra-slice communication utilizes the same control features as inter-slice, some security challenges are similar. However, there are several additional security concerns associated with intra-slice communication, such as 5G user equipment, slice service interfaces, sub-slices, slice manager, and network functions-based security. Some of them are highlighted in Table IV. In the preceding section, we highlighted critical challenges and associated issues within the 5G architecture.

2) Security Threats, Challenges and Issues: Similar to inter-slice communication, 5G user equipment is a major point of attack for intra-slice communication, which can be exploited for unauthorized access to slices or services, as illustrated in Fig. 16. These unapproved accesses may lead to unexpected resource consumption, confidentiality problems, and DoS attacks. The attack that occurs while the service is in communication with the slice is referred to as a slice-service interface attack. The network slice can be compromised if an adversary tries to attack the service which may affect other services utilizing the same slice. Furthermore, sub-slice attacks are concerned with vulnerabilities due to a chain of communication between slices and sub-slices. Hence, if the weakest sub-slice is attacked, all the interconnected slices can be compromised. The slice manager security reflects the trust, mutual authentication, access rights, APIs, and network slice templates when utilizing a service. However, the risks are increased when third-party applications are authorized to manage the network slices. The services that use the network slices might be attacked through network functions such as general cyber-attacks, software attacks, and physical attacks.

3) Related Work: 3GPP reports on NS and security suggest using primary authentication services along with stacked secondary authentication for a 5G user equipment to access a network slice [87]. Primary authentication would allow interconnection among various technologies and roaming, whereas secondary authentication facilitates integration. Olimid and Nencioni suggest implementing security levels and allowing limited rights for third-party applications and users to access a network slice [29]. Furthermore, they also suggest using isolated network slices for common services to enhance security. Kotulski et al. conducted a review of security concerns associated with network slices and concluded that

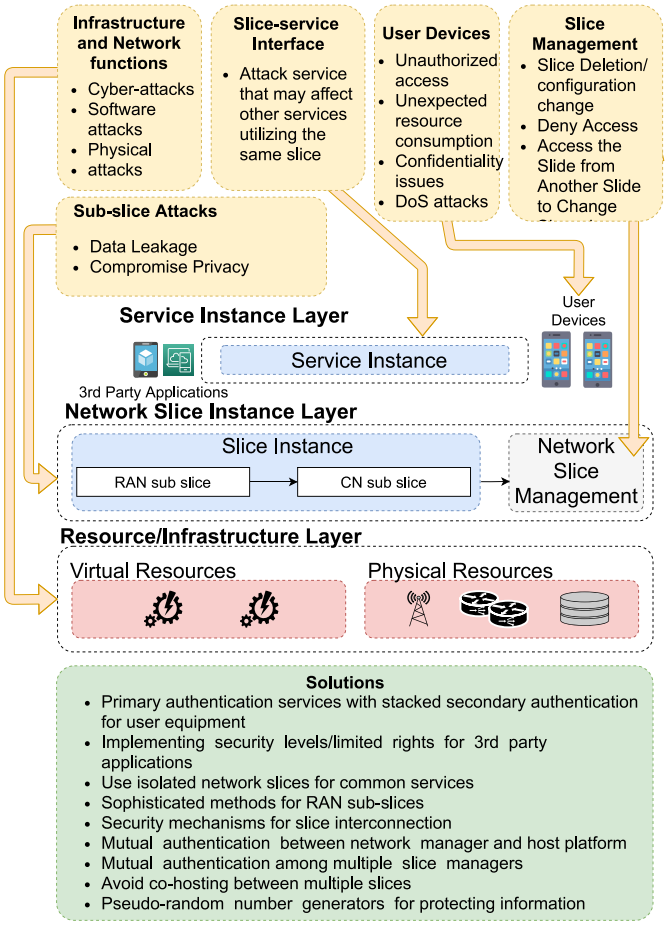

Fig. 16. Intra-Slice Security Threats and Possible Solutions.

sophisticated methods are needed to be developed specifically for RAN sub-slices [79]. This work also suggests implementing security mechanisms for slice interconnection as they are the most vulnerable points of attack. Khan et al. suggested the use of mutual authentication between the network manager and host platform to make the intra-slice communication secure, specifically at slice manager level [4]. Furthermore, if there are multiple slice managers, mutual authentication mechanisms need to be implemented for granting slice access. Furthermore, the NGMN alliance report suggests that the co-hosting between multiple slices should be avoided for improving the services that are dedicated to sensitive applications in order to avoid security mishaps [100]. Bordel et al. mainly focused on the security of the intra-slice domain and proposed the use of pseudo-random number generators for protecting and hiding information such as frequency usage.

4) Countermeasures: Similar to inter-slice security, studies considering intra-slice security make use of authentication and authorization mechanisms along with pseudo-random number generators for protecting information in network slices. Furthermore, attacks propagate through the communication between access points, user equipment, slices, sub-slices, slice manager, and the resource layer. In order to secure slices, E2E security should be considered rather than logical network-based security. Moreover, minimal authenticity, integrity, and confidentiality requirements need to be sent among peers and slices. Also, the service and slice layers should be equipped with lawful interception. The main point of attack in the existing studies was found to be third-party applications. Therefore, each application should undergo a basic security mechanism before being integrated with slices and related services.

D. Slice Broker

1) Introduction: The role of network slice broker (NSB) introduces a new business model to 5G architecture for resource trading between network operators and tenants [112]. Network slice brokering is proposed as a centralized mediator and a controlling entity to provide admission control for incoming resource requests. Initially, a few main use cases are identified as enhancing coverage by operator collaboration, sharing a common core network by multiple RANs, sharing a common RAN by multiple core networks, and sharing network coverage and spectrum.

2) Security Threats, Challenges and Issues: The brokering should have strong Authentication, Authorization, and Accounting (AAA) mechanisms to allow only authentic stakeholders to selectively and securely access the platform. Therefore, at both ends, which are networking tenants and operators, the broker should maintain robust authentication mechanisms to receive the brokering service. If an outsider (attacker) gets access to the system, he can manipulate the broker service and violate the privacy of stakeholders in the system. Each stakeholder (i.e., IoT tenants, MNOs) indicates the requested or offered security level of their system and slices via SSLAs to the network slice broker. Such security information in SSLAs is necessary for slice brokers to select suitable slices with the required security level for each tenant. When different stakeholders share a common platform to share these SSLAs, it is prone to side-channel attacks where competitors get access to the SSLAs of a stakeholder. Therefore, slice brokers should be able to securely store and manage SSLAs. In addition to that, DDoS attacks may occur when a malicious stakeholder (either network tenants or from the operator side) sends several fake requests, which will overload the network slice broker and jeopardize the slice allocation process [82].

3) Related Work: Almost all the work related to security in network slice brokering has a close alliance with blockchain technology. In [113], blockchain is used to build E2E network slices securely with multiple stakeholders involved in the 5G networks. With the integration of blockchain, their solution mainly overcomes the challenges in terms of anonymity, accountability, security, and privacy. In particular, the blockchain-based broker will support secure contract negotiation, secure auctions, secure end-to-end slice creation, and anonymous transactions. As highlighted in [114], the exploitation of permissioned consortium blockchain concepts for brokering will mostly eliminate privacy issues since the stakeholders are known. Here, the concept of slice leasing ledger blockchain is introduced for future factory use cases that require multi-operator slice creation. In [115], the blockchain-based slice brokering framework ensures the

security of transactions for resource requests and resource allocation.

4) Countermeasures: For many brokering solutions in network slicing in the current literature, Blockchain is used as a key enabling technology. Although the concept of network slice brokering has emerged as a promising solution to facilitate dynamic resource trading between resource providers and network tenants, it may encounter some challenges with respect to security. There can be security-related challenges such as AAA issues, secure SLA management, and the possibility of DDoS attacks. Existing research work on network slice brokering does not explicitly address these security aspects and privacy considerations at the tenant and operator ends. Moreover, further work is required on integrating the slice broker in the automated network management when the scalability requirements are increasing.

E. ZSM Security

1) Introduction: In diversified environments and domains, ZSM empower autonomous network systems. Hence, AI/ML, closed-loop networked automation, and API-based attacks are susceptible to attacks on the API level, intent-based interfaces, and autonomous tasks due to their autonomous nature (c.f. Table IV). Some of the critical threats, associated challenges and issues within the 5G core network architectures are discussed below.

2) Security Threats, Challenges and Issues: The APIs in the ZSM framework are responsible for service monitoring, orchestration, management, and provisioning tasks. This makes APIs an eminent target for attackers. A study by Gartner suggests that API attacks will be the most prominent and frequent by 2022 [102]. There are different types of attacks that can be associated at the API level such as parameter, identity, man-in-the-middle, and DoS attacks. Parameter attacks focus on the data that is sent or received by APIs. On the other hand, attacks concerning session tracking, authorization, and authentication are exploited by identity attacks. Unencrypted message communication between APIs provides an opportunity for man-in-the-middle attacks. Furthermore, APIs can be submerged by a large volume of requests which are categorized as DoS attacks [103], [116]. Intent-based interfaces are considered to be the mean of automation in the ZSM architecture. The potential security challenges associated with intent-based interfaces include abnormal behavior, undesirable configuration, and information exposure [103], [116]. Unplanned reboots or application abortion may lead to anomalies in domain orchestration services which provide a window to abnormal behavior attacks. The undesirable configuration mainly concerns the domain orchestration services such as NS [117]. A feedback-driven process (closed-loop management automation) pairs the optimization of resources with intent-based services. Many types of attacks can be associated with this level such as deception, man-in-the-middle, and DoS attacks [118]. AI/ML is the heart of the ZSM architecture which enables the automation of the services, however, there are security concerns related to AI/ML that needs to be tackled. Attack vectors, poisoning attacks, adversarial attacks, and model extraction attacks, are some of the threats associated with AI/ML. These attacks tamper with the training data, steal model parameters to modify them, and add adversarial examples [103], [116].

3) Related Work: ZSM is a relatively new concept. Therefore, only a very few research works are available on focus on its security concerns. Benzaid and Taleb carried out a study on the integration of AI and ZSM networks in the 5G domain and envisioned the use of AI as a key enabling technology while highlighting AI-related security concerns towards ZSM realization [103], [116]. Bonati et al. [119] proposed ZSM-based architecture for cellular networks (CellOS). Most of their work highlights the technical aspects to realize the ZSM in cellular technology, but the study also highlights security-related issues that might compromise the system. Furthermore, Bega et al. focuses on the NS application while using the ZSM architecture for capacity allocation [117]. The study uses deep learning and forecasting models to provide service provisioning while reducing management costs. However, the study highlights the potential threats that can be the basis of data and sensitive information leakage. Carrozzo et al. conducted an in-depth study for the usage of ZSM architecture in multi-operator 5G networks [118]. This study highlights that security threats in ZSM will be one of the challenges in realizing network automation. The study also suggests using distributed ledger techniques (DLT) in the ZSM architecture to ensure the security of the system.

4) Countermeasures: As ZSM is a new concept, existing studies have only highlighted security issues rather than proposing solutions. Although some of the studies use authentication mechanisms, they cannot be considered as an effective solution for ZSM security. Few works have proposed the use of DLT to ensure security but no proof of work has been given to realize the holistic system. ZSM system needs to incorporate encryption techniques and facilitate role-based access control lists at the API level to improve security. Many standardization bodies recommend the use of IETF RFC 5280 certificate compliance integrated with transport layer security protocol to maintain a basic level of security. The standardized bodies also recommend the information be passed through TLS 1.2, a secure transport layer protocol for maintaining confidentiality. The researchers should consider a defensive distillation mechanism, generative adversarial networks for adversarial, block-box, and white-box attacks, and enforcement of API and micro gateways to enhance the level of security in ZSM systems.

F. Other Security Threats

A variety of attacks can affect the performance of NS. Some of the attacks or threats are also associated with the techniques that are used to enhance NS security, such as blockchain technology. One of the attacks that surfaced recently is the parity multi-sig attack. The attack was introduced in 2017 and affected mostly the smart contracts and the wallets associated with it. However, the same can be applied to NS as it can attack the transactions between the slices and the network service provider. The prevention of this attack can be performed

TABLE V
APPLICABILITY OF SECURITY SOLUTIONS TOWARDS SECURITY THREATS, CHALLENGES, AND ISSUES

Threat Vector	Security Solution										Remarks
	AI/ML Security	Security Orchestration	Blockchain	SSLA, Policy Management	Security Monitoring	Slice Isolation	SDN/NFV Security	SbD/ PbD	SECaaS	Security Slice	
Life-cycle Security	M	H	L	M	M	L	H	H	L	H	Authentication and encryption techniques are to avoid fake slice instances. The problem of network slice security during the transmission phase and the data security from the deleted slices are still open issues.
Inter-Slice Security	M	H	M	M	M	H	H	H	L	H	Secure keying schemes and authentication mechanisms have opted for inter-slice security, however, the security associated with the communication between two slices and the independent access control for each slice are still open issues.
Intra-Slice Security	M	H	L	M	M	M	H	H	L	H	Authentication and Authorization mechanisms have been extensively proposed, however, limited work has been carried out on end-to-end slice security using logical networks. Furthermore, 3rd party applications are main point of attacks, therefore, security methods needs to be devised, accordingly.
Slice Broker	M	M	H	M	H	L	L	M	L	L	Security aspects are hardly discussed in slice brokering. The key security aspects include AAA (Authentication, Authorization, and Accounting), SSLA management, and mitigation of Distributed Denial of Service (DDoS) attacks.
ZSM Security	H	H	M	H	H	M	H	M	M	H	Some studies used authentication mechanisms and distributed ledger techniques for solving security issues. The problems regarding defensive distillation mechanism, generative adversarial networks for adversarial, block-box, and white-box attacks and enforcement of API and micro gateways are still required to be devised in order to enhance the level of security in ZSM systems.

by employing external auditors that can inspect the contracts as well as perform formal security checks related to the service initialization. An attack named Destination Advertisement Object (DAO) is quite famous concerning IoT and network slices [94]. The compromised slices in the network might communicate to the slice manager in a periodic manner that can flood the network with messages, which in turn, affects its reliability, latency, and energy efficiency. However, if the DAO attack is initiated at the slices that are connected with other slices, it can totally disrupt the network as all the intermediate slices may be involved in the transmission process. Another kind of attack that is discussed quite rarely is the Sybil attack [120]. Discussed mostly in the context of social networks and the IoT network nodes, the Sybil attack is associated with the mimicking of a node's identity or camouflaging multiple fake identities within a network that can affect the overall trust mechanism, access resources, voting-based applications, and more.

Furthermore, Sybil attacks are very famous for their ability to attack distributed networks. 51 % attack is a fearsome attack related to p2p networks, which occurs when the control of more than 51% of the nodes is acquired by one or more miners/users [29]. The same can be considered for network slices when more than 51% slices are assigned/acquired by a similar group.

V. SECURITY SOLUTIONS AND SERVICES

Considering the security threats, challenges, and issues highlighted in Section IV, this section presents security solutions and services that are available in the literature. The strengths of existing solutions are highlighted while possible improvements are also pointed out. Furthermore, the importance of each of the presented security solutions towards resolving the highlighted security threats, challenges, and issues presented in Section IV is tabulated in Table V.

A. AI/ML Based Security Solutions

1) Introduction: NS enables adding a new layer of abstraction in the design of a 5G service. Even though this added layer of abstraction has its own advantages, it does pose security challenges and risks [121]. As discussed in Section IV, several security issues related to LC, Inter-slice and Intra-slice communication, slice broker, and ZSM, such as DoS, Distributed DOS (DDoS), spoofing of identity, confidentiality, and integrity of the data can be solved through AI/ML-based techniques. This is due to their ability to quickly learn the patterns from existing data and predict/classify anomalies and intrusions. For instance, we can use a traffic performance baseline that controls the behavior of network slices based on the services provided by it. An IoT slice could be used to show the short bursts of traffic and lower usage of the CPU. The ML algorithms can identify changes in the behavior and thus can automatically trigger an alert to search anomalies in the traffic, identifying the recent failed attempts of authentication, that can provide automatic remediation based on the situation. Another use case where AI/ML algorithms can be as a solution for security issues in NS is detecting and stopping the abuse of privileges where AI/ML algorithms can be used to identify the abnormal usage of functions/protocols or abnormal accessing of resources, through which the traffic can be deviated or blocked based on the policies.

The AI/ML techniques can be used to address the following security issues related to NS:

DoS, DDoS, Resource exhaustion: DoS or DDoS attacks can flood the network slice with heavy traffic, thereby exhausting the resources of a network slice. This may lead to the

unavailability of services of a network slice to a customer. These attacks can severely affect the LC of NS, inter and intra-slice communication, slice broker, and ZSM which may lead to the consumption of the resources. AI/ML algorithms can be trained with the traffic data from the network slices to understand the patterns of requests for resources in the slices. Based on this, AI/ML algorithms can identify the requests that aim at DoS/DDoS/resource exhaustion attacks in the network slices in advance, through which the countermeasures can be taken by the MNOs to prevent these attacks [122].

Identity Spoofing: In this security threat, an adversary may use the identity of another entity to access the required services from a network slice. Identity spoofing may severely affect slice broker and ZSM. AI/ML algorithms can be deployed to analyze the behavior patterns of users. If there is a deviation or abnormality from the usual behavioral pattern of the users, their credentials can be revoked [123].

Repudiation Attack: In this security threat, the malicious users' actions can be changed by manipulating authoring information in the log files in the network slice. These attacks may severely hamper the services of LC, inter and intra-slice communication, slice broker, and ZSM. AI/ML approaches can be used to detect these forgeries in the network slices by behavior correlations [124].

Information Disclosure Attacks: In this type of attack, sensitive information of users of the network slice will be unintentionally revealed because of placing the resources at various security levels that may lead the hackers to craft a malicious hack. This attack may jeopardize the LC functioning of NS, inter and intra-slice communication, slice broker, and ZSM. The AI/ML approaches can be used to learn and identify the appropriate placement policies to prevent hackers from gaining access to sensitive information [125].

Intrusion Detection: Intruders may break into NS to gain access and tamper the data/activities at several phases in the LC of an NS, inter and intra-slice communication, slice broker, and ZSM. In order to detect unauthorized users trying to access sensitive data in the network slice to perform different attacks and steal or manipulate data, a strong intrusion detection mechanism has to be designed. By constantly monitoring the network traffic, ML algorithms can be trained to detect intrusions effectively [126].

Security in NS requires monitoring of anomalies or E2E event tracking. The exchanges between the actors across the slices have to be secured by continuous monitoring as it may lead to potential attacks. AI/ML algorithms play a vital role in this context. The smart slice security through AI is depicted in Fig. 17. To deploy protection, AI-based strategies for detection and remediation can be applied. In addition to the basic reporting of the threats from providers, the tenants may deploy their own probes to detect attacks in their slices. Remediation strategies can be applied based on the critical asset knowledge on the tenant side [127].

2) Existing Work/Related Work: Thantharate et al. have developed a model based on neural networks for detecting and thereby eliminating potential threats in a network slice proactively [78]. The proposed model, named as 'Secure5G',

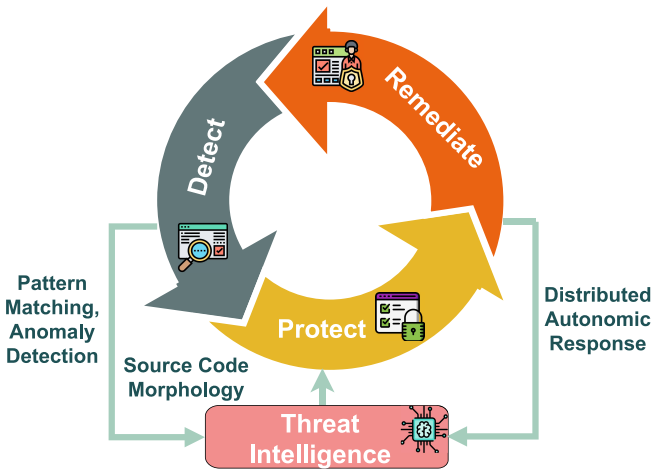

Fig. 17. AI/ML for NS Security.

isolates the potential threats at the network slice before it can spread to the core network and then to the external network. In a similar work, Xie et al. have used lasso regression to analyze the traffic flow of a network slice for a smart home environment to ensure that the traffic flow is valid to secure the home environment [128]. Another interesting work in [129] developed an affordable, resilient and highly secure defense framework based on Moving Target Defence (MTD) principle to minimize defense cost and security vulnerabilities. The authors in this study have proposed to use a network slice integrated with multi-agent deep reinforcement learning for a vehicular network embedded with SDN to deploy an IP shuffling-based MTD. Thus, the IP addresses of nodes are changed dynamically to confuse the intruders/attackers. Furthermore, the presence of an anomaly physical node in a network may result in the degradation of a network slice's performance while exposing sensitive data to intruders/attackers. As a solution, a cooperative anomaly detection mechanism using a hybrid hidden Markov-transfer learning model is presented in [130]. Table VI highlights AI/ML-based security solutions for network slicing.

Summary: Even though AI/ML-based approaches have significant potential to solve security-related issues of NS, there are several challenges that need to be addressed to realize the full potential of AI/ML in NS. Some of the challenges that hinder their adoption for managing the security in NS are data collection, i.e., how much of the data has to be collected, how frequently the data has to be collected, adaptation of the AI/ML models to the ever-changing types of attacks, and black box behavior of the AI/ML models.

B. Security Orchestration

1) Introduction: NS is a dynamic eco-system, which is constantly changing according to user requirements. Similar to other network services, NS security also needs agile and dynamic management. Especially, NS should help maintain the E2E security levels according to the security SLAs and policies. As discussed in Section IV, NS eco-system is facing

TABLE VI
AI/ML-BASED SECURITY SOLUTIONS FOR NETWORK SLICING

Security Threat	Affected Network Slice	Current Approach	Solution provided by AI-ML Approaches
DoS, DDoS, Resource exhaustion	Network Slice LC, Inter and Intra slice communication, slice broker, ZSM	Domain isolation, access to resources based on roles	Countermeasures can be taken as AI/ML approaches can forecast these attacks before happening
Identity Spoofing	Slice broker, ZSM	Authentication, authorization, and accounting	AI/ML algorithms can detect abnormality in the usual behavioral pattern of the users. Their credentials can be revoked in case of abnormalities
Repudiation Attack	LC, inter and intra slice communication, slice broker, and ZSM	Tracking through logs and Authentication, authorization, and accounting; Using certificates to confirm identity	Countermeasures can be taken as AI/ML approaches can be used to detect the forgeries in the network slices by behavior correlations
Information Disclosure Attacks	LC of NS, inter and intra slice communication, slice broker, and ZSM	Access control, mutual authentication, and encryption	The AI/ML approaches can be used to learn to identify the appropriate placement policies to prevent hackers from gaining access to sensitive information
Intrusion Detection	LC of an NS, inter and intra-slice communication, slice broker, and ZSM	Access control, mutual authentication	Countermeasures can be taken as AI/ML approaches can detect the intruders in network slices based on their signatures

many security issues. These security threats can occur anywhere in the network. To mitigate these challenges, new security solutions have to be deployed. Similar to other network functions, these security mechanisms are also deployed as VNFs in network slices. The fast deployment of relevant security VNFs at the correct location/slice with a sufficient amount of resources can eliminate most of these security threats.

However, the amount of network resources available for a network slice is limited and only a certain portion of those resources can be used to operate security resources. Therefore, these limited network resources should be managed efficiently. In this regard, managing the life cycle of the security service and related VNFs play a vital role. Under the life-cycle management, the operational factors such as enabled security functionalities, allocated amount of resources, operational duration and operational location have to be defined by dynamically analyzing the security status of the network.

Existing traditional NSM is responsible for the management of deployed VNFs in a network. However, NSM is not specially designed to analyze security aspects. Most of the existing reference NSMs have been mainly designed without considering security aspects [52]. Therefore, a separate central element called a security orchestrator is important to perform the above security operations in the NS ecosystem independently without being a burden to NSM. The network slicing security orchestrator can perform critical tasks such as security threat detection, dynamic deployment of mitigate mechanisms, security level monitoring, security VNF life-cycle management and optimize the resource utilization for security services. In addition, the use of security orchestration eliminates the requirement of manual or human-centric security management and establishes the way toward security automation. Security automation is a mandatory requirement for slicing systems in future networks due to the high dynamicity and variety of network services.

2) Existing Work/Related Work: A security orchestrator framework for NFV-based systems was defined by ETSI NFV ISG group.[2] Here, the VNF workflow management defined by ETSI NFV MANO [131] has been extended to achieve E2E security orchestration. This ISG group's specification specifies the different functionalities of a security orchestrator. Moreover, a security orchestrator based on ETSI NFV reference architecture was proposed in [132]. In [133], [134], authors have achieved AAA and communication channel protection for IoT systems by leveraging SDN and NFV security orchestrations. A framework to secure virtualized, multi-tenant 5G-based IoT traffic by using an autonomic control loop traffic filtering is proposed in [135]. There are few research work, which focus on security management of SDN/NFV enabled/aware IoT systems [133], [134], [136], [137], [138], [139], [140], [141]. In these research efforts, authors have used the reference architecture developed by ANASTACIA [142] as the baseline to enable dynamic security reaction capabilities. In [143], authors extend the NFV MANO framework to implement a network security manager, which can regulate slice access based on dynamic security policies. The proposed solution can detect the time of security policy violations at slices. In [144], authors propose a high-level architecture for a security orchestrator for a federated NS environment. This architecture is yet to be implemented and tested properly.

Summary: To the best of the authors' knowledge, there is no advanced NS-specific security orchestrator available in the current literature. Thus, the above NFV-based security orchestration framework can be used as a foundation to implement security orchestrators for future NFV systems including NS-based networks.

C. Blockchain Based Solutions

1) Introduction: Blockchain is gaining attention from both academia and the industry due to its tremendous potential in realizing numerous novel applications, such as cryptocurrencies, which are not possible otherwise [145]. Blockchain is a time-stamped collection of blocks of data, which are immutable, i.e., it is practically impossible to modify or delete the data in the blockchain [146], [147]. Cryptographic principles are used to store the data in blocks in the blockchain, which are interconnected with each other. Blockchain is being used to manage the identification, record data, manage interactions, authenticate, register, and validate transactions and assets [148]. Apart from several domains such as healthcare,

[2]https://www.etsi.org/technologies/nfv

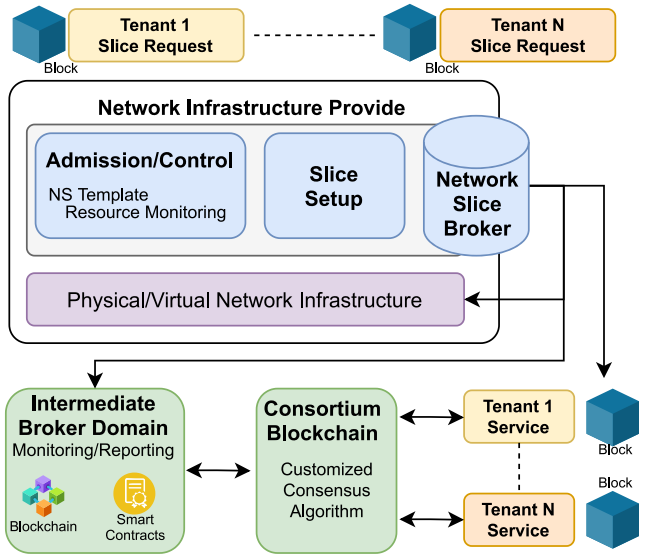

Fig. 18. Blockchain for Slice Brokering.

insurance, and banking, blockchain can also be used in the telecommunication sector for several applications in 5G communication, such as data management, identity-as-a-service, fraud detection, and IoT connectivity [149]. Some of the security issues of NS, such as, alteration of LC slice configurations, tampering with the integrity of slice templates, unauthorized access of slices during inter and intra-slice communication, fake requests by malicious stakeholders in slice broker, poison attacks, and adversarial attacks on AI/ML models in ZSM can be prevented by usage of blockchain. This is through the inherent properties of blockchain including immutability and traceability, which can handle the aforementioned security issues of NS.

2) Existing Work/Related Work: Several research works have predominantly explored the usage of blockchain to address security issues of the network slice broker. For instance, a blockchain-based network slice broker design is proposed by Nour et al. in [113]. The proposed design supports the slice provider in creating E2E slices and also in the selection of resources across several resource providers. A series of smart contracts are envisioned for subslice-deployment brokering mechanisms. Furthermore, a novel solution for network slice brokering that utilizes blockchain, namely, NSBchain, has been proposed by Zanzi et al. in [150]. By using smart contracts, NSBchain enables the infrastructure providers to allocate network resources to the intermediate broker. Through NSBchain, intermediate brokers can allocate and redistribute the resources in an automated, scalable, and secure manner, as depicted in Fig. 18. Furthermore, Valtanen et al. discussed a use case for blockchain-based network-slice-brokering in [151]. The authors discuss a scenario based on industrial automation that acquires the required slices dynamically and autonomously. Moreover, Lin et al. proposed an infrastructure design for slice brokers based on blockchain [152]. In this design, the network slices of registered brokers can be traded in a secure and fair manner. The transactions are sorted and verified by each broker node to improve the accountability of the records in a network slice. The broker nodes are bundled into blocks and are added to a shared ledger that is maintained by every member of the network.

Blockchain is also explored to address the security issues in inter and intra-slice communication by several researchers. Papadakis-Vlachopapadopoulos et al. proposed a blockchain-based solution to enable communication across slices between several domains to automate orchestration [153]. This solution ensures trust between the participating untrusted parties, providing crash-fault tolerance and security, minimal consumption of resources, and managing the communication overheads in intra-slice communication. The authors in [154] proposed a service orchestrator blockchain that uses the automation capabilities of smart contracts for establishing secure intra-slice communication among several tenants.

In addition, when a request is raised for the creation of a network slice from the slice owner, the slice provider uses a network slice template or a blueprint. This template will be translated by the slice provider to meet the specific requirements of the slice, such as radio resources, network resources, and computing resources. Once the E2E slice is created, the slice provider and the vertical sign an SLA. SLAs are also signed between the slice provider and the resource providers. The expectations of customers from a service provider are specified in SLA. Also, an SLA checks whether the service is delivered as per the contract which helps in managing the degradation of Quality of Service (QoS). SLA should also define the requirements of QoS such as latency, throughput, and bandwidth. QoS associated with the predefined types of slices (uRLLC, eMBB, and mMTC) should be reflected in the SLA in 5G [113], [155]. Saad et al. proposed a framework based on blockchain for secured and trusted management of SLA [156]. The objectives of the proposed framework are: (1) monitoring the key performance indicators that are specified in the SLA that is signed between the resource providers and slice provider, and the slice provider and the vertical; (2) confirming if an SLA is violated; (3) compensate the slice provider and the vertical automatically.

Summary: Several research works have explored the utilization of blockchain technologies to address the security issues of slice broker, and intra and inter-slice communication. However, the usage of blockchain as a solution for NS security has its own challenges, such as high energy consumption, slower response rate (latency), difficulty in the scaling of blockchain networks due to consensus, and inefficiency of blockchain to effectively handle some of the attacks including DDoS and 51% attack. These issues should be addressed in order to realize the full benefits of blockchain technology for NS security.

D. SSLA, Policy Management

1) Introduction: Intelligence in future networks should be gathered from continuous monitoring of the involved physical and virtual resources and should be fed to an entity that runs as a policy manager. The role of a security policy manager is particularly devoted to taking actions according

to a pre-defined set of security policies and secure service level agreements (SSLAs) with respect to the network slices. Especially, security monitoring should be focused on the timely detection of security policy violations and abnormal behaviors. SSLA and policy management are going hand-by-hand to enable security and business requirements to drive a fully automated environment where network slices should be managed. SSLAs establish the contracts between operators to assure different levels of security, whereas the security policies enable the formalism and abstraction to enforce those SSLAs in the processes of creating and granting the E2E network slices. The level of abstraction of security policies can be defined as high level or medium level. Security policies can be also generated in a reactive or proactive manner. However, when security policy enforcement is adopted for creating network slices ZSM network architecture, it should incorporate with multi-domain policy delegation concepts for different security management domains. It will be challenging to track the accountability of SSLAs and their implementations only by the security policies.

2) Existing Work/Related Work: Some research outcomes are published about securing network slices using SSLAs and how they are monitored and secured when an entity is aiming to attack. In [157], a network architecture is presented for integration of E2E network slices with SSLAs together with the assistance of NSM and security manager. Continuous monitoring for SSLA violation is required for E2E secure slices. The authors of [158] demonstrate the use of SSLAs to secure virtual resources of vehicular network slice. They continuously assess the SSLAs deployed in vehicle-to-everything (V2X) use-case to evaluate the vehicle's trustworthiness. In the INSPIRE-5Gplus [159] project, there is a proposed work for an SSLA manager, which is running in the ZSM architecture to cater to secure network slices. The security management in inter-slice communication needs to consider the inherent security attributes of the communication services [160]. In [160], a mathematical model is presented to specify E2E network slices based on pre-defined policies with security constraints. Although the authors claim that the model is extensible for any access control model deployed in any application service, further investigations are required to prove its applicability to 5G and beyond 5G use cases.

Summary: SSLA and policy management are mandatory to gain intelligent and automated slice monitoring and slice management in the future cognitive networking architecture. This includes the monitoring of SSLA violations in continuing E2E network slice operations and then triggering the corresponding entities to take required actions.

E. Security Monitoring - Analytics, Data Collection

1) Introduction: In network slicing, several virtual networks will be built on a shared platform or infrastructure, which will be used by various devices and users. It is therefore logical that these virtual networks will pose several challenges to NSM to monitor everything in intra-slicing, and inter-slicing. If NSM cannot effectively detect and/or monitor each breakdown or issue, then the concept of sharing resources in NS may create more security and other issues (e.g., device, network, or user behavior) in inter and intra-slicing. Therefore, security monitoring (i.e., data collection and analytics) is one of the potential solutions in NS. Such secure monitoring can prevent unauthorized abuses and loss of business by ensuring that the secure data monitoring or policies are being appropriately implemented in inter or intra-network slicing. Security monitoring can be mainly divided into three categories: (i) management security monitoring, (ii) service security monitoring, and (iii) system security monitoring, as shown in Fig. 19. These approaches may monitor many parts of NS including inter or intra-network slice communication [161], [162]. Following the ESTI document, management security monitoring of NVF in NS can be done using behavior monitoring, attack monitoring, and security policy monitoring. Whereas, service security monitoring mainly contains the monitoring of the service interface that can be monitored and audited in NFV scenarios. Also, in the NFV environment, system security monitoring can be monitored for system integrity, system logs, and traffic monitoring.

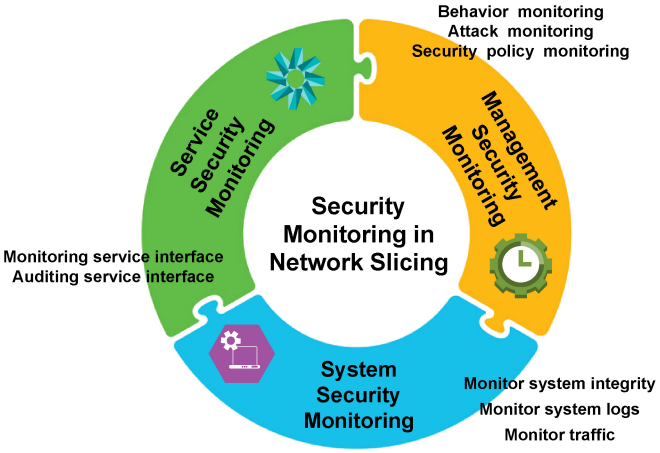

Fig. 19. Categorization of Security Monitoring in NS.

2) Existing Work/Related Work: Management security monitoring: To implement behavior monitoring in NS, Wang et al. proposed a Digital Twin (DT) that can securely monitor the network behavior in NS [163]. The authors proposed a graph neural network-based approach that captures and monitors the relationship between various slices, and resource utilization and measures E2E performance under different network topologies. The DT is being used to realize the vision of automation and security monitoring of network slicing. In another research, Liu et al. proposed a learning-assisted technique that can detect attacks in NS and can also monitor DoS attacks [164]. The authors claimed that a network operator can deploy a learning-based algorithm to detect malicious attacks and can achieve security monitoring in NS. The proposed algorithm learns step-by-step slice performance and enhances the allocation of resources between nodes and slices. In addition, the algorithm reduces the impact of DoS attacks while the performance of the network slice can be retrieved by approximately 98%. Celdrán et al. [165] proposed

a policy-based approach to manage the NS in mobile communication. The authors integrated the basic concepts of NFV and NS and defined the network slice ontology. In the policy-based security monitoring, several metrics have been used, for instance, packet loss frequency (*PktLossFreq*), CPU efficiency (*CPUEff*), and sustained system performance (*SSP*). In addition, an automation policy engine is suggested that would trigger the decisions about the management of slices in intra or inter-slice networks [165].

Service security monitoring: In [136], the authors proposed a security management architecture (called ANASTASIA) that can enable several service-level interfaces which may detect the attacks in NVF in IoT-based critical infrastructure (IoTCI). A few of the service interfaces are the SDN-oriented security enforcement plane interface, NVF-oriented security enforcement plane interface, and IoT-oriented security enforcement plane interface. ANASTASIA includes several threat countermeasures, such as vFirewall, vAAA, and vIoTHoneyNet.

System security monitoring: In [166], Afolabi et al. proposed a new architecture that can enable several features in NS in a 5G network. One example is the instantiation and management of E2E network slicing. The proposed architecture mainly described the multi-slicing in 5G, how they can work together, and how to manage them. In order to monitor the system security, the authors exploited the dynamic policy stack which can monitor several components in the NVF (or intra or inter-slicing) systems. Few of the components include *EventLog* (these are the outstanding events that are basically captured from the server), and *Analytics* (it can generate more complex data and can provide root cause analysis, if any component is failed in NS) [166].

Summary: The concept of slicing includes the implementation of virtual functions, application services, and resource sharing via the softwarization, therefore it requires extensive security monitoring mechanisms to run every part or component of the network, smoothly. Preliminary research have been addressed towards security monitoring, service security monitoring, and system security monitoring, taking into account auditing services, monitoring system integrity, policy monitoring, etc.

F. Slice Isolation

1) Introduction: Slice isolation is one of the key requirements to ensure the security of NS based 5G and beyond networks. Slice isolation requires an NS instance to be completely isolated from other NS instances while utilizing network resources and communicating throughout the mobile network [105]. However, in the practical implementation, slice isolation may occur at different stages in the network in order to increase the utilization of shared network resources, as illustrated in Fig. 20. Strong slice isolation ensures that the information available in one slice instance is not accessible to other slices. Furthermore, a security attack on one or more slice instances will not impact other slice instances and the overall functionality of the network [52]. There can be multiple approaches towards achieving network slice isolation at different levels based on the requirement [79]. For instance, resource

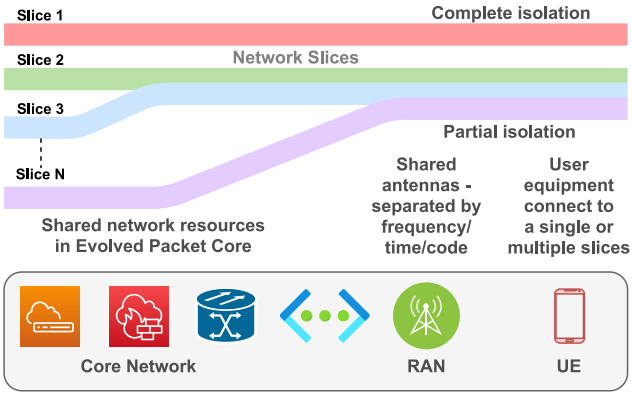

Fig. 20. Different Levels of Network Slice Isolation.

isolation utilizes a set of resources configured to be isolated within the network. This can be achieved through ring-fencing of network and security resources to ensure that the operation of one slice instance will not consume the resource allocated for another slice instance. In addition, communication between different slice instances can be blocked or kept at a minimal level with strict security protocols. Moreover, isolation in the communication network ensures secure signaling and communication between the slice, the network orchestrator and other NSMs. Communication among different elements within the NS should also be secured. Slice isolation can also be performed based on various other aspects such as operating system, language, virtual machine, and sandbox through virtual local area networks, virtual private networks, and tagged network packets.

2) Existing Work/Related Work: Reference [167] introduces several approaches to provide slice isolation for third-party services such as verticals (e.g., industry 4.0) in 5G Mobile Networks to ensure the protection of sensitive information. This is based on establishing a combination of private and public network infrastructure. Accordingly, establishing a private 5G network is the most secure method of isolation while providing a private network on-site and an off-site roaming facility through the MNO, banking on a security protocol such as EPS AKA [168]. However, this protocol does not isolate the traffic from the MNO. Therefore, Extensible Authentication Protocol (EAP) based authentication protocols are proposed, where authentication is performed between the user and the private network of the third party service [167]. Another method proposed in [167] is to deploy a private 5G network utilizing a slice of the MNO radio access network. Furthermore, a gateway core network is proposed for applications such as critical IoT, which does not own a specific geographic location but needs slice isolation to protect sensitive information. In addition, establishing strong slice isolation towards increasing the network resilience against DDoS attacks is presented in [105]. A mathematical model is proposed to provide slice isolation in an on-demand fashion while not exceeding the required E2E delay. Furthermore, [105] elaborates that even though inter-slice isolation provides strong resource isolation, resource utilization is less efficient. In contrast, a better compromise between

network security and resource utilization efficiency is provided by intra-slice isolation. In addition, [169] proposes an implicit mutual authentication and key establishment with service group anonymity (IMAKE-GA) protocol, which also ensures strong slice isolation by establishing a secure key among network components. Furthermore, generating network slices in the 5G core network while satisfying E2E delay constraints and intra-slice isolation requirements is presented in [170]. This work allocates VNFs for core network slices optimally using Mixed-Linear Integer Programming (MILP). These concepts are promising for improving network slice isolation. However, considerable research and development work and testing are still required towards integrating these proposed technologies with existing network protocols and ensuring efficient and seamless network operation. In addition, instead of banking on ML, Federated Learning (FL) can be used to perform various operations within the scope of the network slice [171]. This will keep raw data within the network slice and trained models can be communicated to other slices if required.

Summary: Slice isolation is a key requirement to ensure NS security and privacy. This ensures complete isolation of information among multiple network slices while protecting network slices against threats and attacks of other slices. However, more research and development work is yet to be performed to ensure strong slice isolation while ensuring seamless and efficient network operation.

G. Security-by-Design/Privacy-by-Design

1) Introduction: The concepts of Security-by-Design (SbD) and Privacy-by-Design (PbD) are originally coming from software engineering and considering the very early stage of software design. SbD and PbD can assure the foundation of the final product, software, or service by eliminating and minimizing the possible and anticipated security vulnerabilities and privacy breaches. For instance, certain cloud-based software services are using SbD to automate security by establishing reliable operation of controls and enabling continuous real-time auditing. Particularly in Network Slicing, SbD, and PbD approaches can be exploited in the design of network slices including the relevant VNFs and other resource allocations considering security and privacy as foundation principles. During the slice creation process within a multi-operator multi-tenant platform, it is important to use a design that maintains proper slice isolation mechanisms and attack mitigation techniques.

2) Existing Work/Related Work: There is not much literature that uses SbD and PbD approaches for securing and enabling privacy in NS in an explicit form. However, SbD and PbD are identified as promising research directions in NS security [21]. At the design stage of automating the orchestration of E2E network slices and managing their life-cycle, the level of security can be taken as a key requirement [172]. In [173], Li et. al. present a secure 5G core network slice provisioning mechanism based on a multi-criteria decision-making method. The security issues in NS are analyzed for formulating the secure 5G core network slice provisioning problem as an Integer Linear Programming (ILP) model. Moreover, in [174] the authors model 5G network slice provisioning as an optimization problem and assure security by partially or completely isolating network slices with dedicated network functions.

Summary: The concepts of SbD and PbD are already adopted from the software design to the network design. Both are considered two fundamental design principles in future networks, especially in network slice creation, slice provisioning, and slice resource allocation in multi-party environments. Although the work is initiated, there is plenty of room to evolve the applicability of SbD and PbD in NS security and privacy.

H. Security as a Service

1) Introduction: 5G and beyond networks interconnect a diverse set of IoT-based verticals such as smart vehicles, smart cities smart grids, smart healthcare services, and smart factories. However, most of these IoT devices do not support cutting-edge security features due to various reasons. First, IoT devices have limited computing and storage resources. As a result, a complete security mechanism can not be implemented in these devices [175]. Second, IoT devices have limited energy and these devices are designed to avoid energy-hungry operations. Typically, heavy cryptographic algorithms-based security services consume a significant amount of resources at the run time. Thus, IoT devices eliminate such security services [176]. Third, the IoT deceives lack proper security standardization [177]. As a result, most of IoT devices do not support the standard security features in mobile networks. Fourth, IoT device manufacturers do not implement security functions in their devices. There are two reasons for that. Small-scale IoT device manufacturers might not have enough security expertise and resources to implement advanced security features in their IoT devices. On the other hand, large-scale IoT providers willingly eliminate the implementation of security functions to keep the cost of IoT devices at a minimum. In addition, the security services at the IoT level are not always trustworthy. Mainly, because most of the IoT devices do not follow proper security testing procedures at the manufacturing plants. This decreases the reliability of IoT device level security measures [178].

2) Existing Work/Related Work: To mitigate these challenges, security for IoT devices can be implemented at the network level. Moreover, many vertical operators do not have up-to-date security expertise to manage security aspects of their network [179]. NS can be used as a solution to mitigate these challenges. An NS-based Security-as-a-Service (SECaaS) approach is a viable solution to provide tailor-made security services for IoT devices and vertical network operators. Traditional security services such as AAA services, security monitoring, security event management, security attacks, and intrusion detection can be implemented with a SECaaS approach [180].

Several research work has focused on the deployment of SECaaS with NS technology. In [181], authors propose an NS-based application-aware SECaaS framework for

5G networks. The proposed framework is designed by leveraging SDN and NFV technologies. It can secure the user network traffic by deploying on-demand basis security services at network slices. In [182], authors propose another SDN and NFV-based framework to manage the traffic steering in slicing and deploying security VNFs as a Security Service to satisfy the demands of tenants. Furthermore, a measurable network security metric is defined in [183], where this metric can be used to trigger the deployment of SECaaS at the network slice. The paper also investigates the possibility of deploying proactive security mechanisms such as Moving Target Defense (MTD) a slice-based SECaaS.

Summary: SECaaS concepts are widely used in other technology platforms such as cloud and MEC systems. However, the NS-based SECaaS framework is still at a trivial stage compared to those platforms. Moreover, NS-based SECaaS frameworks need to support automation to cope with the scalability and dynamicity of future mobile networks. Especially, ZSM concepts should be adapted to support full automation. By extending the proposed work in [183], AI techniques can be used to deploy not only reactive but also proactive security services via network slices.

I. Other Security Solutions

1) Dedicated Security Slice: Similar to creating a slice to cater to the requirements of specific network services, a dedicated slice can be deployed to deliver the security functionalities at the system level. This security slice offers system-level security services so that other slices can obtain security via this slice. Thus, each network slice can eliminate the deployment of security solutions while all the resources available for security can be pooled together to deploy advanced security services [6], [42]. This approach is particularly interesting for resource constraint environments, such as private network-based hospitals, factories, and shopping malls [184], [185]. In addition, this is a viable solution during disaster recovery situations.

2) QKD and Quantum-Safe Security: Attacks from quantum computers can make existing standard key exchange algorithms, such as RSA and Diffie-Hellman, vulnerable. Quantum Resistant Algorithms (QRA) and Quantum Key Distribution (QKD) are possible solutions to avoid such threats from quantum computers. NS can be used to control the quantum encryption to effectively defend against attacks from quantum computers by integrating QKD and QRA [186]. Several research works, as seen in [187], [188], [189], have applied QKD in 5G networking experimentally on the Bristol City 5G UK Test Network. Authors in [190] have demonstrated proof-of-transit for the 5G network using QKD on the Madrid Quantum Network. Moreover, Wright et al. [191] have proposed to control the type of encryption (AES+Diffie-Hellman, AES+QKD, AES+QRA) dynamically when data packets in 5G networks will have different security requirements.

A summary of related work for security solutions and services is presented in TABLE VII.

VI. Trust and Privacy in Network Slicing

Privacy and trust are two important aspects to consider under the umbrella of security in NS. Although they are two different domains, yet there exists a close alliance with the security and the related technologies.

A. Trust in Network Slicing

Trust is a paramount property to consider in both 5G and beyond 5G systems in general. In particular, NS has a close alliance with trust as an implicit assurance of its security-related considerations. In a zero-trust network, the devices should undergo an access control mechanism while joining the network to obtain any sort of service. In a way, trust in the NS framework can be considered the expectation of users to avoid security threats while using NS services. This includes the same threat vectors which are identified in Section III with respect to LC security, inter and intra-slice security, slice broker security, and ZSM security. In another way, the trust in NS can be evaluated to the extent of the network slices meet the user security requirements including the key security goals described in Section III (i.e., mutual authentication, confidentiality, integrity, authorization, and availability).

In particular, as NS supports multi-operator cooperation it is important to ensure the trust among the MNOs as well. In principle, NS enables multiple MNOs to deploy different services on top of the shared physical infrastructure allowing inter-operator resource sharing. In the resource-sharing relationship in NS, the MNOs may play the role of Resource Providers (RPs) as well as resource users (tenants). On one hand, an RP MNO may provide slicing services to another tenant MNO with a monitoring interface, where the tenant has to trust RP in accordance with an agreed SLA. This can be further established with the Security SLAs with the predefined security levels. On the other hand, RP MNO acts as a physical infrastructure provider, where the tenant has more control over VNF management and orchestration. Here the tenant has better visibility and needs to trust RP for sharing common network functions and maintaining the security goals of NS. Therefore, a dynamic and efficient trust-relationship model should be carefully maintained for the multi-operator cooperation in 5G and beyond. When the network slices are created and granted to the end users, they can be certified by a Trust Reputation Manager (TRM). The trust reputation assessment can be performed based on the historical behavior of virtual and physical networking elements. In order to demonstrate a multi-domain policy enforcement ecosystem in the network slices, the trustworthiness can be evaluated to take the decisions.

B. Privacy Aspects in Network Slicing

The key privacy goals in NS may include user privacy, data privacy, and anonymity in the 5G echo system. On the other hand, we identify that certain threat vectors mentioned in Section III are related to the possible privacy violations in the NS architecture. For instance, the threats for inter-slice and intra-slice security may directly affect the privacy issues with respect to user and data privacy (see Fig. 21).

TABLE VII
SUMMARY OF RELATED WORK FOR NS SECURITY SOLUTIONS AND SERVICES

Ref.	Key Contributions	Security Solutions								Applications							
		AI/ML	Security Orchestration	Blockchain	SSLA,policy management	Monitoring & Analytics	Slice Isolation	SbD/PbD	Security As a Service	Smart Transportation	Industrial Automation	Smart Home & City	Military Applications	UAVs & Drones	massive IoT	Telecom and Networks
[78]	Develops a model, "Secure5G' based on neural networks for detecting and thereby eliminating the potential threats proactively in a network slice	✓				✓									✓	
[124]	Discusses how AI techniques can be applied to network security and network slicing.	✓														✓
[125]	Presents an edge-centric IoT defense scheme to detect, identify, classify and mitigate IoT DDoS attacks.	✓										✓			✓	
[126]	Utilize signal-to-noise ratio trace in IEEE 802.11ad networks for efficient physical-layer spoofing attack detection.	✓														✓
[127]	Explore how to address the security of ML-based systems using existing threat modeling and attack libraries	✓									✓					
[128]	Reviews applications and design aspects of intelligent reflecting surfaces	✓												✓	✓	✓
[129]	Proposes a hybrid principal component analysis - firefly-based ML model to classify intrusion detection system datasets	✓														✓
[130]	Provides a brief overview of smart slice security with AI and software-defined security	✓														✓
[131]	Uses lasso regression to analyze the traffic flow of a network slice for a smart home environment to ensure that the traffic flow is valid to secure the home environment	✓				✓						✓				
[132]	Develops an affordable, resilient and highly secure defence framework based on moving target defence (MTD) principle to minimize defence cost and security vulnerabilities.	✓				✓				✓			✓			
[133]	Designs a cooperative anomaly detection mechanism by using a hybrid hidden Markov-transfer learning model.	✓				✓									✓	
[135]	A security orchestrator based on ETSI NFV reference architecture was proposed		✓													✓
[136]	A novel framework based on policy is proposed to AAA and security functions for Channel Protection in SDN and NFV-enabled IoT networks		✓												✓	✓
[137]	A novel security framework that is cyber-situational aware and policy-based is proposed for dynamic and continuous AAA and also functions for virtual security for Channel Protection in SDN/NFV-enabled IoT networks.		✓												✓	✓
[138]	Proposes a security framework to secure virtualized, multi-tenant 5G-based IoT traffic by using an autonomic control loop traffic filtering.		✓												✓	
[139]	Proposes an architectural design to capture the challenges related to security and privacy of IoT-critical infrastructures and cyber-physical systems and enable them to take autonomous decisions related to security by using SDN/NFV technologies.		✓			✓									✓	
[140]	A novel policy-based framework is designed to exploit the security features of NFV/SDN.		✓												✓	✓
[141]	A novel framework to exploit SDN/NFV-based security feature integration with IoT security		✓												✓	
[142]	A novel mechanism that leverages NFV and SDN to deploy and enforce the honeynets in IoT autonomously		✓												✓	
[143]	Proposes deployment of virtual firewalls automatically by leveraging NFV MANO for protecting narrow band-IoT mMTC communications.		✓												✓	✓
[146]	Extends the NFV MANO framework to implement a network security manager which can regulate the slice access based on dynamic security policies.		✓													✓
[147]	Proposes high-level architecture for a security orchastrator for federated network slicing environment.		✓													✓
[156]	Introduces a blockchain-based solution for automated orchestration for cross slice communication		✓	✓												✓
[157]	Proposes a novel blockchain-based service orchestrator utilizing smart contracts to establish cross-service communication among network slices		✓	✓												✓
[116]	Proposes blockchain-based broker design to provide a mechanism that secures and ensures anonymous transactions.			✓												✓
[153]	A novel solution for network slice brokering that uses a blockchain-based technology, NSBchain, has been proposed through which intermediate broker can allocate and redistribute the resources in an automated, scalable, and secure manner			✓												✓
[154]	Discusses a use case for blockchain-based network-slice-brokering for industrial automation that required slices dynamically and autonomously			✓							✓					
[155]	Proposes an infrastructure design for slice brokers based on blockchain, where, the network slices of registered brokers can be traded in a secure and fair manner.			✓												✓
[159]	Proposes a blockchain based trust architecture to automatically manage the SLAs			✓	✓											✓
[160]	A network architecture is presented for integration of E2E network slices with SSLAs with the assistance of NSM and security manager.				✓											✓
[161]	Demonstrates the use of SSLAs to secure virtual resources of vehicular network slice to evaluate the vehicle trustworthiness.				✓					✓						
[163]	Presents a mathematical model to specify E2E network slices based on pre-defined policies with security constraints.				✓											✓
[166]	Proposes a DT that can securely monitor the network behaviour in NS.					✓					✓					
[167]	Proposes a learning-assisted technique that can detect the attack in NS and can monitor denial of service attack.					✓				✓						
[168]	Proposes policy-based approach to manage the NS in mobile communication by integrating the basic concepts of NFV and NS.					✓										✓
[139]	Proposes a security management architecture that can enable several service-level interfaces which may detect the attacks in NVF in Internet of Things based critical infrastructure					✓									✓	
[169]	Proposes a new architecture that can enable several features like instantiation and management of E2E NS in 5G network.					✓										✓
[170]	Introduces several approaches to provide slice isolation for third party services like industry 4.0 in 5G Mobile Networks to ensure the protection of sensitive information.						✓				✓					
[107]	A solution is proposed to mitigate DDoS attacks proactively in 5G core network slicing using slice isolation.						✓									✓
[195]	A security architecture towards multi-tenant SDN/NFV enabled access networks was presented that includes policy-based security management, service monitoring, service analytics, and virtual security functions towards improving network security.															✓
[196]	A SDN/NFV-enabled ZSM security management framework to facilitate UAV applications is proposed													✓		
[176]	Presents a secure 5G core network slice provisioning mechanism based on a multi-criteria decision-making method.							✓								✓
[177]	5G network slice provisioning as an optimization problem is modeled and security is assured by partially or completely isolating network slices with dedicated network functions.							✓								✓
[184]	Proposes a NS based application-aware SECaaS framework for 5G networks.								✓							✓
[185]	Proposes a SDN and NFV based framework to manage the traffic steering in slicing and deploy security VNFs as a Security as a Service to satisfy the demands of tenants.								✓							✓
[186]	Investigates the possibility of deploying proactive security mechanisms such as Moving Target Defense (MTD) a slice based SECaaS.								✓							✓

By definition of network slicing, tenants share common resources, where a slight information leak may create serious privacy violations in terms of user and data privacy by making threats on both inter-slice and intra-slice scenarios. One of the most common privacy issues arises with NS, with its close alliance of IoT use cases and the extremely large data sets they collect [44]. When there is an information leakage even between the slices, that may introduce serious privacy violations by making a threat to inter-slice communication. This is a key motivation to have anonymity as a privacy goal in NS. In such situations, robust slice isolation mechanisms with well-protected inter-slice communication via the

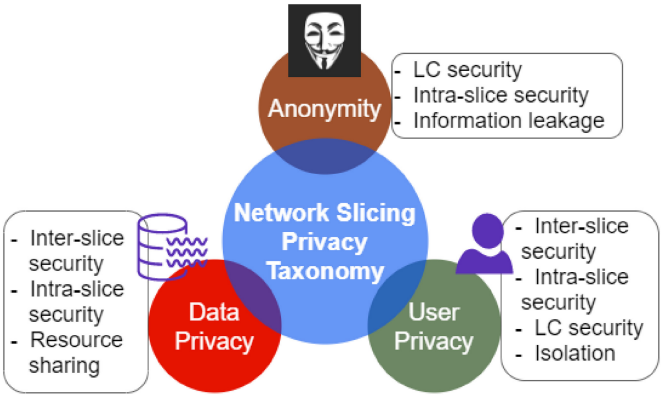

Fig. 21. Privacy Taxonomy in NS.

secured channels are needed to preserve the user and data privacy [21].

When we consider different application areas, such as mission-critical V2X scenarios, they may need real-time privacy-preserving mechanisms to mitigate the privacy risks that create LC security threats. In a way, NS may also provide solutions to enhance privacy by isolating networking resources to a specific set of users. However, the specification of the network slice and the LC may include to which extent the slice identification and the correlation to customer devices will assure the privacy of individual users.

C. Solutions for Privacy and Trust in NS

For developing trust-ensuring solutions for NS, blockchain-like distributed ledger technologies are identified with a greater potential [46], [194]. Blockchain can be used to generate trust among different operators and other stakeholders and allow collaboration among them to deploy secure E2E network slices. These network slices can be certified with a certification tool in such a way as to be trusted by all peers. Trusted blockchain-based network slices will explicitly provide distributed trust in a zero-trust network architecture.

A combination of AI and distributed ledger technologies can create a technological platform for accountability where the decisions taken by the algorithms can be recorded in a trusted distributed ledger. This may exploit to develop consistent security policies among the network slice tenants to ensure trust. The lack of transparency in the processing segments of many deep learning algorithms may create more issues in exploring model uncertainty and transparency. In such a circumstance, to achieve human trust in AI-empowered services related to NS in future networks, a trusted broker can be incorporated [47].

Hardware-based Trusted Execution Environments (TEEs) are also used to achieve integrity and confidentiality in the networking field to bring the hardware-based root of trust. They may provide remediation to mitigate certain NS-related attacks, such as side channel attacks [195].

Privacy can be also considered with respect to the different resource allocation mechanisms in NS [196]. This may create privacy threats in slice brokering as well. In the shared-based approach, tenant information leakages may occur while allocating the total budget at individual nodes. In the reservation-based approach, a privacy violation may occur only when the information is leaked by the system while accepting or rejecting the resource requests. Introducing privacy isolation with privacy rules can be also taken as another mechanism that can be used to directly influence the data plane by managing encryption of the slice services [45], [197]. This may allow isolating privacy dynamically for different privacy levels' required information. The detailed solutions for privacy and trust in NS are presented in Table VIII.

VII. Lessons Learned and Future Research Directions

This section discusses the lessons learned from existing NS-related research work. Furthermore, based on the lessons learned, possible future research directions are synthesized toward paving the path to realize secure and privacy-preserving NS in 5G and beyond networks. Important lessons learned and future research directions on network slicing are also highlighted in Fig. 22.

A. Threat Modeling

1) Lessons Learned: In order to mitigate security concerns related to network slices, cryptographical methods need to be integrated to maintain authenticity, integrity, and confidentiality in slice templates that could secure both the storage and transmission characteristics. Furthermore, the system designer should opt for E2E security for network slices as they are E2E logical networks. In this regard, the rendering of private AI can be leveraged to secure both the data and transmission parameters in network slices. The main characteristic is to secure the transmission parameters, which can be performed through homomorphic encryption that performs the desired operations while the data or parameters are in encrypted form, making the manipulation difficult for the interceptors. Practices such as certificateless cryptography and public key infrastructure can also be used for secure communication between network slices. The guidelines provided in ISO/IEC 62443 standard that undertake the network capabilities and high-level application requirements can be considered to design the defence against network management attacks in network slices. Dynamic isolation mechanisms with the help of AI and optimization strategies can also be designed to cope with inter-slice communication-related attacks for improving global security policy.

2) Open Research Questions:

- How to strengthen the security of NS through NS life-cycle, inter-slice communication, intra-slice communication, slice broker, and zero-touch network and management systems?
- How to use AI and ML efficiently towards behavioral analysis, anomaly detection, and end-to-end slice isolation?
- How to isolate network slices with heterogeneous network infrastructure and devices
- How to create trust between slice manager and network slices?

TABLE VIII
SUMMARY OF RELATED WORK FOR PRIVACY AND TRUST IN NETWORK SLICING

Ref.	Key Contributions	Privacy	Trust	Threats Vectors					
				Life-cycle Security	Inter-Slice Security	Intra-Slice Security	Slice Broker Security	ZSM Security	Federated Slice Security
[201]	This work proposes a trust model for NS which uses a cloud model algorithm to compute the network slice subjective trust value.		✓	✓					
[111]	This proposes a security approach for network slicing-based 5G architectures that uses security trust zones. Here the security trust zone concept is analyzed by a profiling methodology taking into account the characteristics of the supported network slice.		✓	✓					
[202]	This proposes group anonymous privacy preserving mutual authentication (PPMA) and privacy-preserving one-way authentication (PPOA) protocols to address the privacy issues in NS.	✓		✓					
[199]	The authors study resource allocation mechanisms in NS and consider the impact of privacy in each approach.	✓			✓	✓			
[44]	This work provides a framework for privacy-preserving slice selection for IoT devices in 5G networks with network slices and based on their service types. Moreover, the framework enables anonymous service access for IoT devices from third-party service providers without revealing their service access behavior.	✓		✓					
[203]	This paper presents a model-free resource scheduling scheme for 5G network slicing, in which the user-related privacy data is not used for decision-making. Deep Convolutional Neural Network (CNN) is adopted to model the complex 5G network environment and solve the optimization challenge caused by the lack of a precise model.	✓						✓	
[204]	This work proposes two fully-distributed algorithms to the unique equilibrium without revealing privacy-sensitive parameters from the slice tenants. The privacy-preserving, low-complexity, near-optimal distributed algorithm for RAN network slicing will enable the MVNOs selfishly compete with each other.	✓		✓		✓			
[45], [200]	The authors use the NS concept to formulate a solution for Non-Public Networks in e-health applications which require quality of service and privacy between slices. The blockchain-based solution is used to secure the network slice management layer to assure reliability and data integrity.	✓			✓				
[205]	This work identifies the use of blockchain, smart contracts, and AI to design a trusted and efficient federated slicing architecture.		✓				✓	✓	✓
[206]	The paper proposes a lightweight trust-based framework for node authentication in wireless personal area networks (WPANs) using NS.		✓						
[47]	For mission-critical and safety operations may require transparent AI-based decision makings and quantifiable quality-of-trust (QoT). In this work, the authors identify the concept of trustworthy autonomy for 6G with explainable AI (XAI) to create qualitative and quantitative trust.		✓	✓				✓	
[146]	This work uses authorization and access control functions for NS deployments with closed-loop network management. The management and orchestration (MANO) security functions are extended with usage control capabilities to regulate the access control and use of network slices to trusted entities only.		✓	✓				✓	
[207]	The article introduces the smart, trustworthy, and liable 5G security architecture proposed in INSPIRE-5Gplus project [162]. They discuss advanced mechanisms of assuring trust using software entities of TEEs, digital rights management approaches (DRMs), labeling schemes, and AI-powered validation tools.		✓					✓	
[64]	This paper presents a design of a liability-aware security management system for network slice management in multi-party and multi-layer 5G architecture. They use the concept of security-by-contracts. Trust and reputation management system is one component of their system that assess the trustworthiness of information captured by the system.		✓					✓	

3) Possible Future Directions: AI is a promising technique for performing functions, such as behavioral analysis and anomaly detection, to provide end-to-end isolation of network slices. It is apparent that handling heterogeneous devices is a challenging task in any network environment. However, it can also affect the level of security that needs to be attained. The design of methods that can perform slice isolation with heterogeneous devices would greatly improve the security of network slices. Furthermore, software-defined mobile network controller (SDM-C) and software-defined mobile network coordinator (SDM-X) can also be used for the management and orchestration of heterogeneous devices using multiple slices in a single instance. The role of the slice manager is quite vital in not only improving the network functionalities but also creating intermediary communication services between tenants and network management. The methods that can evaluate the trust of the network slices within the slice manager functionalities would also help in improving its security.

- End-to-end isolation of network slices using AI techniques can be considered for mitigating end-to-end security issues.
- Methods that can perform slice isolation with heterogeneous environments at different levels should be designed to improve security.

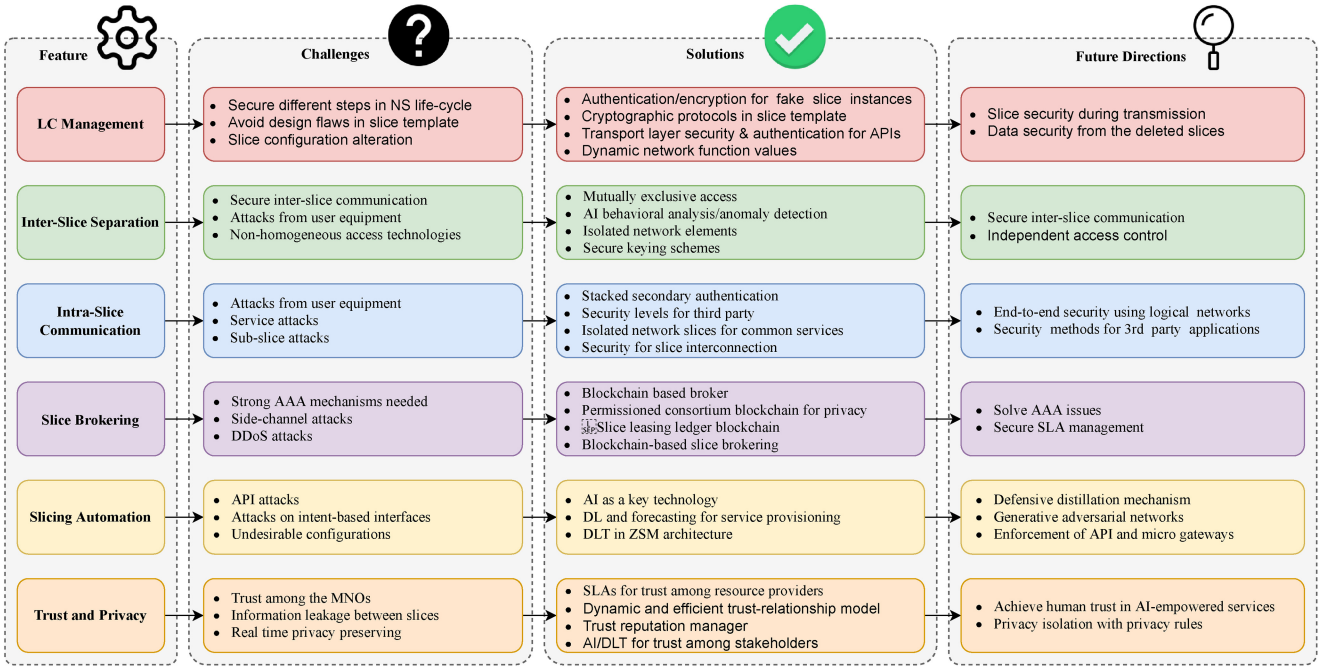

Fig. 22. Important Lessons Learnt and Future Research Directions on NS

- The exploration of software-defined mobile network controller (SDM-C) and software-defined mobile network coordinator (SDM-X) should be used for the management and orchestration of network slices.
- Methods that can evaluate the trust of the network slices should be designed to improve the slice manager functionalities.
- Secondary authentication and customer device isolation should be performed to increase network slice security.

B. Security Solutions

1) Lessons Learned: Designing security solutions and services to overcome NS security threats and challenges is an essential requirement for realizing NS-enabled 5G and beyond networks. Many AI/ML-based security solutions and services are being developed to identify and resolve attacks ranging from DoS, identity spoofing, and identity spoofing to intrusion detection. In addition, security orchestration establishes security automation in NS. Furthermore, blockchain-based security solutions are developed to solve issues, such as alteration of NS LC, tampering integrity of slice templates, and attacks on AI/ML models in ZSM. Moreover, SSLA and policy management also play an important role in multi-domain policy management when creating network slices for ZSM architecture. Also, security monitoring, analytics, data collection solutions, slice isolation techniques, and SDN/NFV-based security solutions also play a pivotal role in NS security. In addition, NS-based SECaaS to provide tailor-made security solutions, and dedicated security slices to offer system-level security services are also developed to enhance the security in NS.

2) Open Research Questions:

- How to implement NS security solutions without compromising network performance?
- How to perform NS-specific security orchestration?
- How to perform extensive security monitoring across all the parts of an NS-enabled network?
- How to ensure security and privacy with AI/ML-based solutions?

3) Possible Future Directions: The development of security solutions and services to secure NS highlights multiple research directions. For instance, ensuring data security and privacy when utilizing AI/ML-based solutions and developing NFV-based security orchestration frameworks are key research directions to ensure NS security. Furthermore, blockchain-based security solutions can be made more energy efficient, faster, and more secure towards increasing NS security. Also, applying SSLAs to secure virtual resources in network slices, and novel methods for analytics and data collection for security monitoring is essential in terms of improving NS. In addition, strong slice isolation techniques using authentication methods that do not hinder network performance are being developed. Moreover, SDN/NFV-based security solutions ranging from firewall deployment, access control lists, traffic direction, traffic segmentation, intrusion detection and prevention, and deep packet inspection to SDN/NFV-based ZSM security management techniques are being developed to establish NS security. While security-by-design, privacy-by-design, and security as a service are emerging as promising approaches towards NS security, allocating dedicated security slices to offer security functionalities at the system level is also being investigated.

C. Trust and Privacy

1) Lessons Learned: In addition to security, trust, and privacy are two important topics to be discussed under the umbrella of NS. However, in the current literature, there is

a very limited amount of work available with a key focus on trust and privacy in NS. When the NS technology is achieved with the participation of multiple MNOs, it is significant to maintain the trust for sharing physical and virtual infrastructure. Blockchain-like DLT-based solutions have been mostly exploited in bringing trust to NS applications. At the same time, when the common resources are shared between different network slices, it is important to maintain the isolation of tenant information to prevent any information leakage and privacy violation.

2) Open Research Questions:

- How to ensure trust in NS in complex multi-operator mobile networks?
- How can blockchain be used for NS security in a zero-trust network architecture?
- How to preserve patient privacy with NS while performing functions, such as slice brokering?

3) Possible Future Directions: In order to bring intelligent trust-enabling mechanisms with NS, there is great potential for incorporating AI/ML-based solutions to evaluate trust in a quantitative manner. Particularly, since the next-generation network management is going to be more intelligent and automated, trust in the NS architecture can be considered a metric to evaluate the stakeholders including tenants and resource providers. The level of trust can be considered a key value indicator (KVI) for next-generation networks. PbD approaches can be used during the design stage of network slices to keep the proper slice isolation and isolate the privacy of the users. Use of homomorphic encryption and differential privacy mechanisms to manage tenant information related to NS architecture. It is also important to develop these trust-enabling technologies and privacy-enhancing mechanisms related to NS in a scalable manner in such a way as to support the network and application heterogeneity.

VIII. Conclusion

This paper provides a comprehensive survey of the attacks, security threats, security challenges, security issues, security solutions, and research directions of NS security. The paper formulates a taxonomy for NS security and privacy, which sets the structure for the rest of the paper. Key NS attack scenarios are discussed to provide an in-depth understanding of the security and privacy vulnerabilities in NS-enabled networks. Furthermore, the paper discusses NS security challenges and issues, such as NS life-cycle security, inter-slice security, intra-slice security, slice broker security, and ZSM security, In addition, the paper presents possible security solutions, ranging from AI/ML security, security orchestration, and blockchain to introducing a dedicated slice for security towards mitigating the identified security issues. We present the co-relation of these solutions with identified threats via related research work. We also present NS trust and privacy aspects related to NS. Furthermore, gaps in existing research and development work are highlighted while possible future research directions in NS security and privacy are presented along with a taxonomy for NS security. It is envisaged that this paper would facilitate research and development work that would ultimately contribute towards realizing a secure NS framework in future mobile communication networks.

References

[1] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May/Jun. 2020.

[2] M. Shafi et al., "5G: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1201–1221, Jun. 2017.

[3] B. Li, M. Zhang, Y. Rong, and Z. Han, "Transceiver optimization for wireless powered time-division duplex MU-MIMO systems: Non-robust and robust designs," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 4594–4607, Jun. 2022.

[4] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8792139/

[5] P. Rost et al., "Mobile network architecture evolution toward 5G," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 84–91, May 2016.

[6] P. Porambage and M. Liyanage, "Security in network slicing," *Wiley 5G Ref: Essential 5G Reference Online*, vol. 2019, pp. 1–12, May 2020.

[7] R. H. Jhaveri, S. V. Ramani, G. Srivastava, T. R. Gadekallu, and V. Aggarwal, "Fault-resilience for bandwidth management in industrial software-defined networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 3129–3139, Oct.-Dec. 2021.

[8] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on software-defined networking," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 27–51, 1st Quart., 2015.

[9] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 90–97, Feb. 2015.

[10] Y. Dinitz, S. Dolev, S. Frenkel, A. Binun, and D. Khankin, "Network cloudification," in *Proc. Int. Symp. Cyber Security Cryptogr. Mach. Learn.*, 2019, pp. 249–259.

[11] S. Wang, J. Xu, N. Zhang, and Y. Liu, "A survey on service migration in mobile edge computing," *IEEE Access*, vol. 6, pp. 23511–23528, 2018.

[12] A. ur Rehman Khan, M. Othman, S. A. Madani, and S. U. Khan, "A survey of mobile cloud computing application models," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 393–413, 1st Quart., 2013.

[13] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for Internet of Things realization," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2961–2991, 4th Quart., 2018.

[14] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5G: Survey and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 94–100, May 2017.

[15] V. A. Cunha et al., "Network slicing security: Challenges and directions," *Internet Technol. Lett.*, vol. 2, no. 5, 2019, Art. no. e125.

[16] R. Islambouli, Z. Sweidan, and S. Sharafeddine, "Dynamic multipath resource management for ultra reliable low latency services," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, 2019, pp. 987–992.

[17] S. Mishra and N. Mathur, "Load balancing optimization in LTE/LTE-A cellular networks: A review," 2014, *arXiv:1412.7273*.

[18] C. de Alwis, H. K. Arachchi, A. Fernando, and M. Pourazad, "Content and network-aware multicast over wireless networks," in *Proc. 10th Int. Conf. Heterogen. Netw. Qual. Rel. Security Robustness*, 2014, pp. 122–128.

[19] C. de Alwis, H. K. Arachchi, V. De Silva, A. Fernando, and A. Kondoz, "Robust video communication using random linear network coding with pre-coding and interleaving," in *Proc. 19th IEEE Int. Conf. Image Process.*, 2012, pp. 2269–2272.

[20] R. Ratasuk, N. Mangalvedhe, Y. Zhang, M. Robert, and J.-P. Koskinen, "Overview of narrowband IoT in LTE Rel-13," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2016, pp. 1–7.

[21] S. Wijethilaka and M. Liyanage, "Survey on network slicing for Internet of Things realization in 5g networks," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 957–994, 2nd Quart., 2021.

[22] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 74–80, Feb. 2014.

[23] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.

[24] R. Islambouli and S. Sharafeddine, "Autonomous 3D deployment of aerial base stations in wireless networks with user mobility," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, 2019, pp. 1–6.

[25] *Description of Network Slicing Concept*, NGMN Alliance, Frankfurt, Germany, 2016, pp. 1–7.

[26] "Study on management and orchestration of network slicing for next generation network," 3GPP, Sophia Antipolis, France, 3GPP Rep. TR 28.801, 2017.

[27] S. Redana et al., *5G PPP Architecture Working Group: View on 5G Architecture* 5G PPP, Heidelberg, Germany, 2019.

[28] Z. Sweidan, R. Islambouli, and S. Sharafeddine, "Optimized flow assignment for applications with strict reliability and latency constraints using path diversity," *J. Comput. Sci.*, vol. 44, Jul. 2020, Art. no. 101163.

[29] R. F. Olimid and G. Nencioni, "5G network slicing: A security overview," *IEEE Access*, vol. 8, pp. 99999–100009, 2020.

[30] A. Mathew, "Network slicing in 5G and the security concerns," in *Proc. 4th Int. Conf. Comput. Methodol. Commun. (ICCMC)*, 2020, pp. 75–78.

[31] M. Chahbar, G. Diaz, A. Dandoush, C. Cérin, and K. Ghoumid, "A comprehensive survey on the E2E 5G network slicing model," *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 1, pp. 49–62, Mar. 2021.

[32] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018.

[33] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Comput. Netw.*, vol. 167, Feb. 2020, Art. no. 106984.

[34] A. Blenk, A. Basta, M. Reisslein, and W. Kellerer, "Survey on network virtualization hypervisors for software defined networking," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 655–685, 1st Quart., 2016.

[35] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 4th Quart., 2021.

[36] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on multi-access edge computing security and privacy," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1078–1124, 2nd Quart., 2021.

[37] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and challenges of software-defined mobile networks in network security," *IEEE Security Privacy*, vol. 14, no. 4, pp. 34–44, Jul./Aug. 2016.

[38] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.

[39] R. Dangi, A. Jadhav, G. Choudhary, N. Dragoni, M. K. Mishra, and P. Lalwani, "ML-based 5G network slicing security: A comprehensive survey," *Future Internet*, vol. 14, no. 4, p. 116, 2022.

[40] F. Salahdine, Q. Liu, and T. Han, "Towards secure and intelligent network slicing for 5G networks," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 23–38, 2022.

[41] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 80–87, May 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7926921/

[42] *5G Security Recommendations Package# 2: Network Slicing*, NGMN Alliance, Frankfurt, Germany 2016, pp. 1–12.

[43] S. Wijethilaka and M. Liyanage, "Realizing Internet of Things with network slicing: Opportunities and challenges," in *Proc. IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2021, pp. 1–6.

[44] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, pp. 644–657, Mar. 2018.

[45] J. P. de Brito Gonçalves, H. C. de Resende, R. da Silva Villaca, E. Municio, C. B. Both, and J. M. Marquez-Barja, "Distributed network slicing management using blockchains in E-health environments," *Mobile Netw. Appl.*, vol. 26, pp. 2111–2122, Oct. 2021.

[46] M. A. Togou et al., "DBNS: A distributed blockchain-enabled network slicing framework for 5G networks," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 90–96, Nov. 2020.

[47] C. Li, W. Guo, S. C. Sun, S. Al-Rubaye, and A. Tsourdos, "Trustworthy deep learning in 6G-enabled mass autonomy: From concept to quality-of-trust key performance indicators," *IEEE Veh. Technol. Mag.*, vol. 15, no. 4, pp. 112–121, Dec. 2020.

[48] S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 111–117, Jun. 2019.

[49] Y. Wu, H.-N. Dai, H. Wang, Z. Xiong, and S. Guo, "A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1175–1211, 2nd Quart., 2022.

[50] "An introduction to network slicing." Accessed: Nov. 6, 2022. [Online]. Available: https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf

[51] "Study on management and orchestration of network slicing for next generation network (release 15) v15.10," 3GPP, Sophia Antipolis, France, 3GPP Rep. TR 28.801, 2018.

[52] X. Li et al., "Network slicing for 5G: Challenges and opportunities," *IEEE Internet Comput.*, vol. 21, no. 5, pp. 20–27, Sep./Oct. 2017.

[53] X. Shen et al., "AI-assisted network-slicing based next-generation wireless networks," *IEEE Open J. Veh. Technol.*, vol. 1, pp. 45–66, 2020.

[54] S. Huang, B. Guo, and Y. Liu, "5G-oriented optical underlay network slicing technology and challenges," *IEEE Commun. Mag.*, vol. 58, no. 2, pp. 13–19, Feb. 2020.

[55] "Optus notifies customers of cyberattack compromising customer information." 2022. Accessed: Nov. 7, 2022. [Online]. Available: https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack

[56] "5G network slicing vulnerability: Location tracking attacks." 2021. Accessed: Nov. 6, 2022. [Online]. Available: https://blog.adaptivemobile.com/5g-network-slicing-vulnerability-location-tracking-attacks

[57] "GSMA security." 2022. Accessed: Nov. 6, 2022. [Online]. Available: https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme

[58] T. Flynn, G. Grispos, W. Glisson, and W. Mahoney, "Knock! knock! who is there? investigating data leakage from a medical Internet of Things hijacking attack," in *Proc. 53rd Hawaii Int. Conf. Syst. Sci.*, 2020, pp. 1–10.

[59] T. Wichary, J. Mongay Batalla, C. X. Mavromoustakis, J. Żurek, and G. Mastorakis, "Network slicing security controls and assurance for verticals," *Electronics*, vol. 11, no. 2, p. 222, 2022.

[60] C. M. Mohammed and S. K. Shaikhah, "A survey and analysis of architecture and models of network slicing in 5G," in *Proc. 8th Int. Eng. Conf. Sustain. Technol. Develop. (IEC)*, 2022, pp. 192–198.

[61] L. Waked, M. Mannan, and A. Youssef, "The sorry state of TLS security in enterprise interception appliances," *Digit. Threats Res. Pract.*, vol. 1, no. 2, pp. 1–26, 2020.

[62] D. Diemert and T. Jager, "On the tight security of TLS 1.3: Theoretically sound cryptographic parameters for real-world deployments," *J. Cryptol.*, vol. 34, no. 3, pp. 1–57, 2021.

[63] D. D. Siqueira Braga, M. Niemann, B. Hellingrath, and F. B. De Lima Neto, "Survey on computational trust and reputation models," *ACM Comput. Surveys*, vol. 51, no. 5, pp. 1–40, 2018.

[64] C. Gaber et al., "Liability-aware security management for 5G," in *Proc. IEEE 3rd 5G World Forum (5GWF)*, 2020, pp. 133–138.

[65] R. Kumar and R. Sharma, "Leveraging blockchain for ensuring trust in IoT: A survey," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8599–8622, 2021.

[66] B. Chen et al., "A security awareness and protection system for 5G smart healthcare based on zero-trust architecture," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10248–10263, Jul. 2021.

[67] B. W. Cramer, "Not over my backyard: The regulatory conflict between 5G rollout and environmental and historic preservation," *Digit. Policy Regulat. Govern.*, vol. 23, no. 2, pp. 97–112, 2021.

[68] T. Mumtaz, S. Muhammad, M. I. Aslam, and N. Mohammad, "Dual connectivity-based mobility management and data split mechanism in 4G/5G cellular networks," *IEEE Access*, vol. 8, pp. 86495–86509, 2020.

[69] L. Wan, Z. Guo, and X. Chen, "Enabling efficient 5G NR and 4G LTE coexistence," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 6–8, Feb. 2019.

[70] A. Delmade et al., "Performance analysis of analog IF over fiber fronthaul link with 4G and 5G coexistence," *J. Opt. Commun. Netw.*, vol. 10, no. 3, pp. 174–182, Mar. 2018.

[71] P. Suthar, V. Agarwal, R. S. Shetty, and A. Jangam, "Migration and interworking between 4G and 5G," in *Proc. IEEE 3rd 5G World Forum (5GWF)*, 2020, pp. 401–406.

[72] C. Marquez, M. Gramaglia, M. Fiore, A. Banchs, and X. Costa-Perez, "Resource sharing efficiency in network slicing," *IEEE Trans. Netw. Service Manag.*, vol. 16, no. 3, pp. 909–923, Sep. 2019.

[73] G. Wang, G. Feng, T. Q. Quek, S. Qin, R. Wen, and W. Tan, "Reconfiguration in network slicing—Optimizing the profit and performance," *IEEE Trans. Netw. Service Manag.*, vol. 16, no. 2, pp. 591–605, Jun. 2019.

[74] "A slice in time: Slicing security in 5G core networks." Nov. 2021. Accessed: Jun. 23, 2022. [Online]. Available: https://www.adaptivemobile.com/security-insights/reports

[75] N. Alliance. "5G security recommendations package #2: Network slicing." 2016. Accessed: Jul. 20, 2022. [Online]. Available: https://www.ngmn.org/publications/5g-security-recommendations-package-2-network-slicing.html

[76] "A slice in time: Slicing security in 5G core networks—White paper." Accessed: Jul. 2, 2022. [Online]. Available: https://info.adaptivemobile.com/network-slicing-security

[77] N. A. E. Kuadey, G. T. Maale, T. Kwantwi, G. Sun, and G. Liu, "DeepSecure: Detection of distributed denial of service attacks on 5G network slicing—Deep learning approach," *IEEE Wireless Commun. Lett.*, vol. 11, no. 3, pp. 488–492, Mar. 2022.

[78] A. Thantharate, R. Paropkari, V. Walunj, C. Beard, and P. Kankariya, "Secure5G: A deep learning framework towards a secure network slicing in 5G and beyond," in *Proc. 10th Annu. Comput. Commun. Workshop Conf. (CCWC)*, 2020, pp. 852–857.

[79] Z. Kotulski et al., "On end-to-end approach for slice isolation in 5G networks. Fundamental challenges," in *Proc. Federat. Conf. Comput. Sci. Inf. Syst. (FedCSIS)*, 2017, pp. 783–792. [Online]. Available: https://fedcsis.org/proceedings/2017/drp/228.html

[80] R. A. Addad, T. Taleb, H. Flinck, M. Bagaa, and D. Dutra, "Network slice mobility in next generation mobile systems: Challenges and potential solutions," *IEEE Netw.*, vol. 34, no. 1, pp. 84–93, Jan./Feb. 2020.

[81] S. Rani, H. Babbar, G. Srivastava, T. R. Gadekallu, and G. Dhiman, "Security framework for Internet-of-Things-based software defined networks using blockchain," *IEEE Internet Things J.*, vol. 10, no. 7, pp. 6074–6081, Apr. 2023.

[82] T. Hewa, A. Kalla, P. Porambage, M. Liyanage, and M. Ylianttila, "How DoS attacks can be mounted on network slice broker and can they be mitigated using blockchain?" in *Proc. IEEE 32nd Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, 2021, pp. 1525–1531.

[83] K. Cao et al., "Improving physical layer security of uplink NOMA via energy harvesting jammers," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 786–799, 2020.

[84] K. Cao et al., "Enhancing physical-layer security for IoT with nonorthogonal multiple access assisted semi-grant-free transmission," *IEEE Internet Things J.*, vol. 9, no. 24, pp. 24669–24681, Dec. 2022.

[85] M. Devi and A. Majumder, "Side-channel attack in Internet of Things: A survey," in *Proc. Appl. Internet Things (ICCCIOT)*, 2021, pp. 213–222.

[86] J. Cáceres-Hidalgo and D. Avila-Pesantez, "Cybersecurity study in 5G network slicing technology: A systematic mapping review," in *Proc. IEEE 5th Ecuador Tech. Chapt. Meeting (ETCM)*, 2021, pp. 1–6.

[87] "System architecture for the 5G system; stage 2 (release 16) v16.4.0," 3GPP, Sophia Antipolis, France, 3GPP Rep. TS 23.501, 2020.

[88] P. Rost et al., "Network slicing to enable scalability and flexibility in 5G mobile networks," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 72–79, May 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7926920/

[89] *Huawei: 5G Security Architecture White Paper*, Huawei, Shenzhen, China, 2017.

[90] A. Kaloxylos, "A survey and an analysis of network slicing in 5G networks," *IEEE Commun. Stand. Mag.*, vol. 2, no. 1, pp. 60–65, Mar. 2018.

[91] P. Rost et al., "Customized industrial networks: Network slicing trial at hamburg seaport," *IEEE Wireless Commun.*, vol. 25, no. 5, pp. 48–55, Oct. 2018.

[92] A. Ksentini and P. A. Frangoudis, "Toward slicing-enabled multi-access edge computing in 5G," *IEEE Netw.*, vol. 34, no. 2, pp. 99–105, Mar./Apr. 2020.

[93] B. Chafika, T. Taleb, C.-T. Phan, C. Tselios, and G. Tsolis, "Distributed ai-based security for massive numbers of network slices in 5G & beyond mobile systems," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, 2021, pp. 401–406.

[94] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, "Addressing the DAO insider attack in RPL's Internet of Things networks," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 68–71, Jan. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8510812/

[95] J. Wang and J. Liu, "Secure and reliable slicing in 5G and beyond vehicular networks," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 126–133, Feb. 2022.

[96] Y. Li, X. Zhang, X. Xu, and X. Tao, "Secure network slicing deployment in edge computing," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, 2021, pp. 97–102.

[97] B. Bordel, A. B. Orúe, R. Alcarria, and D. Sánchez-De-Rivera, "An intra-slice security solution for emerging 5G networks based on pseudo-random number generators," *IEEE Access*, vol. 6, pp. 16149–16164, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8315003/

[98] S. Zeb, A. Mahmood, S. A. Hassan, M. J. Piran, M. Gidlund, and M. Guizani, "Industrial digital twins at the nexus of NextG wireless networks and computational intelligence: A survey," *J. Netw. Comput. Appl.*, vol. 200, Apr. 2022, Art. no. 103309. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804521002988

[99] P. Porambage, Y. Miche, A. Kalliola, M. Liyanage, and M. Ylianttila, "Secure keying scheme for network slicing in 5G architecture," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2019, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8931330/

[100] "Security aspects of network capabilities exposure in 5G," NGMN Alliance, Frankfurt, Germany, Rep. GB 918713901, 2019.

[101] "Study on security aspects of 5G network slicing management (release 15) v15.0.0," 3GPP, Sophia Antipolis, France, 3GPP Rep. TR 3.811, 2018.

[102] *How to Build an Effective API Security Strategy*, Gartner, Stamford, CT, USA, 2017.

[103] C. Benzaid and T. Taleb, "AI-driven zero touch network and service management in 5G and beyond: Challenges and research directions," *IEEE Netw.*, vol. 34, no. 2, pp. 186–194, Mar./Apr. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8994961/

[104] A. Mahmood et al., "Industrial IoT in 5G-and-beyond networks: Vision, architecture, and design trends," *IEEE Trans. Ind. Informat.*, vol. 18, no. 6, pp. 4122–4137, Jun. 2022.

[105] D. Sattar and A. Matrawy, "Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, 2019, pp. 82–90.

[106] R. F. Olimid and G. Nencioni, "5G network slicing: A security overview," *IEEE Access*, vol. 8, pp. 99999–100009, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9099823/

[107] T.-H. Ting, T.-N. Lin, S.-H. Shen, and Y.-W. Chang. "Guidelines for 5G end to end architecture and security issues." Dec. 2019. [Online]. Available: http://arxiv.org/abs/1912.10318.

[108] "3GPP TR 33.813: Study on security aspects of network slicing enhancement." Accessed. Jun. 16, 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3541

[109] J. Cao et al., "A survey on security aspects for 3GPP 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 170–195, 1st Quart., 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8894379/

[110] D. Schinianakis, R. Trapero, D. S. Michalopoulos, and B. G.-N. Crespo, "Security considerations in 5G networks: A slice-aware trust zone approach," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2019, pp. 1–8.

[111] *ENISA Threat Landscape for 5G Networks-Threats Assessment for the Fifth Generation of Mobile Telecomunications Networks (5G)*, ENISA, Athens, Greece, 2019.

[112] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From network sharing to multi-tenancy: The 5G network slice broker," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 32–39, Jul. 2016.

[113] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Moungla, "A blockchain-based network slice broker for 5G services," *IEEE Netw. Lett.*, vol. 1, no. 3, pp. 99–102, Sep. 2019.

[114] J. Backman, S. Yrjölä, K. Valtanen, and O. Mämmelä, "Blockchain network slice broker in 5G: Slice leasing in factory of the future use case," in *Proc. Internet Things Bus. Models Users Netw.*, 2017, pp. 1–8.

[115] Y. Gong, S. Sun, Y. Wei, and M. Song, "Deep reinforcement learning for edge computing resource allocation in blockchain network slicing broker framework," in *Proc. IEEE 93rd Veh. Technol. Conf. (VTC-Spring)*, 2021, pp. 1–6.

[116] C. Benzaid and T. Taleb, "ZSM security: Threat surface and best practices," *IEEE Netw.*, vol. 34, no. 3, pp. 124–133, May/Jun. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8994962/

[117] D. Bega, M. Gramaglia, M. Fiore, A. Banchs, and X. Costa-Perez, "AZTEC: Anticipatory capacity allocation for zero-touch network slicing," in *Proc. IEEE Conf. Comput. Commun.*, Jul. 2020, pp. 794–803. [Online]. Available: https://ieeexplore.ieee.org/document/9155299/

[118] G. Carrozzo et al., "AI-driven zero-touch operations, security and trust in multi-operator 5G networks: A conceptual architecture," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2020, pp. 254–258. [Online]. Available: https://ieeexplore.ieee.org/document/9200928/

[119] L. Bonati et al., "CellOS: Zero-touch softwarized open cellular networks," *Comput. Netw.*, vol. 180, Oct. 2020, Art. no. 107380. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S138912862030503X

[120] R. Gunturu. "Survey of sybil attacks in social networks." Apr. 2015. [Online]. Available: http://arxiv.org/abs/1504.05522.

[121] L. Suárez, D. Espes, P. Le Parc, F. Cuppens, P. Bertin, and C.-T. Phan, "Enhancing network slice security via artificial intelligence: Challenges and solutions," in *Proc. Conf. C&ESAR*, 2018, pp. 1–16.

[122] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, "Flowguard: An intelligent edge defense mechanism against IoT DDoS attacks," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9552–9562, Oct. 2020.

[123] N. Wang, L. Jiao, P. Wang, W. Li, and K. Zeng, "Machine learning-based spoofing attack detection in MmWave 60GHz IEEE 802.11 ad networks," in *Proc. IEEE Conf. Comput. Commun.*, 2020, pp. 2579–2588.

[124] C. Wilhjelm and A. A. Younis, "A threat analysis methodology for security requirements elicitation in machine learning based systems," in *Proc. IEEE 20th Int. Conf. Softw. Qual. Rel. Security Companion (QRS-C)*, 2020, pp. 426–433.

[125] M. Gong, Y. Xie, K. Pan, K. Feng, and A. K. Qin, "A survey on differentially private machine learning," *IEEE Comput. Intell. Mag.*, vol. 15, no. 2, pp. 49–64, May 2020.

[126] S. Bhattacharya et al., "A novel PCA-firefly based XGBoost classification model for intrusion detection in networks using GPU," *Electronics*, vol. 9, no. 2, p. 219, 2020.

[127] "5G network slicing and security." Accessed: Nov. 6, 2022. [Online]. Available: https://sdn.ieee.org/newsletter/january-2018/5g-network-slicing-and-security

[128] F. Xie, D. Wei, and Z. Wang, "Traffic analysis for 5G network slice based on machine learning," *EURASIP J. Wireless Commun. Netw.*, vol. 2021, no. 1, pp. 1–15, 2021.

[129] S. Yoon et al., "Moving target defense for in-vehicle software-defined networking: IP shuffling in network slicing with multiagent deep reinforcement learning," in *Proc. Artif. Intell. Mach. Learn. Multi-Domain Operat. Appl. II*, vol. 11413, 2020, Art. no. 114131U.

[130] W. Wang, Q. Chen, X. He, and L. Tang, "Cooperative anomaly detection with transfer learning-based hidden Markov model in virtualized network slicing," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1534–1537, Sep. 2019.

[131] "Network functions virtualisation (NFV); management and orchestration," ETSI, Sophia Antipolis, France, Rep. ETSI GS NFV-MAN 001 V1.1.1 (2014–12), 2017.

[132] B. Jaeger, "Security orchestrator: Introducing a security orchestrator in the context of the ETSI NFV reference architecture," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 1255–1260.

[133] A. M. Zarca, D. Garcia-Carrillo, J. B. Bernabe, J. Ortiz, R. Marin-Perez, and A. Skarmeta, "Managing AAA in NFV/SDN-enabled IoT scenarios," in *Proc. Global Internet Things Summit (GIoTS)*, 2018, pp. 1–7.

[134] A. Molina Zarca, D. Garcia-Carrillo, J. Bernal Bernabe, J. Ortiz, R. Marin-Perez, and A. Skarmeta, "Enabling virtual AAA management in SDN-based IoT networks," *Sensors*, vol. 19, no. 2, p. 295, 2019.

[135] P. Salva-Garcia, J. M. Alcaraz-Calero, Q. Wang, J. B. Bernabe, and A. Skarmeta, "5G NB-IoT: Efficient network traffic filtering for multitenant IoT cellular networks," *Security Commun. Netw.*, vol. 2018, Dec. 2018, Art. no. 9291506.

[136] A. M. Zarca et al., "Security management architecture for NFV/SDN-aware IoT systems," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8005–8020, Oct. 2019.

[137] A. M. Zarca, J. B. Bernabe, I. Farris, Y. Khettab, T. Taleb, and A. Skarmeta, "Enhancing IoT security through network softwarization and virtual security appliances," *Int. J. Netw. Manag.*, vol. 28, no. 5, 2018, Art. no. e2038.

[138] I. Farris et al., "Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2017, pp. 169–174.

[139] A. M. Zarca, J. B. Bernabe, A. Skarmeta, and J. M. A. Calero, "Virtual IoT honeynets to mitigate cyberattacks in SDN/NFV-enabled IoT networks," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1262–1277, Jun. 2020.

[140] P. Salva-Garcia, E. Chirevella-Perez, J. B. Bernabe, J. M. Alcaraz-Calero, and Q. Wang, "Towards automatic deployment of virtual firewalls to support secure mMTC in 5G networks," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2019, pp. 385–390.

[141] J. Gong and A. Rezaeipanah, "A fuzzy delay-bandwidth guaranteed routing algorithm for video conferencing services over SDN networks," *Multimedia Tools Appl.*, vol. 82, pp. 25585–25614, Jul. 2023.

[142] "Anastacia." Accessed: Jun. 16, 2021. [Online]. Available: http://www.anastacia-h2020.eu/

[143] B. Martini et al., "Pushing forward security in network slicing by leveraging continuous usage control," *IEEE Commun. Mag.*, vol. 58, no. 7, pp. 65–71, Jul. 2020.

[144] S. Wijethilaka and M. Liyanage, "Security orchestration framework for federated network slicing," in *Proc. Joint Eur. Conf. Netw. Commun. (EuCNC) 6G Summit*, 2021, pp. 1–2.

[145] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[146] B. Prabadevi et al., "Toward blockchain for edge-of-things: A new paradigm, opportunities, and future directions," *IEEE Internet Things Mag.*, vol. 4, no. 2, pp. 102–108, Jun. 2021.

[147] T. R. Gadekallu et al., "Blockchain for edge of things: Applications, opportunities, and challenges," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 964–988, Jan. 2022.

[148] A. Chaer, K. Salah, C. Lima, P. P. Ray, and T. Sheltami, "Blockchain for 5G: Opportunities and challenges," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2019, pp. 1–6.

[149] T. Hewa, A. Braeken, M. Ylianttila, and M. Liyanage, "Multi-access edge computing and blockchain-based secure Telehealth system connected with 5G and IoT," in *Proc. 8th IEEE Int. Conf. Commun. Netw. (IEEE ComNet)*, 2020, pp. 1–6.

[150] L. Zanzi, A. Albanese, V. Sciancalepore, and X. Costa-Pérez, "NSBchain: A secure blockchain framework for network slicing brokerage," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2020, pp. 1–7.

[151] K. Valtanen, J. Backman, and S. Yrjölä, "Creating value through blockchain powered resource configurations: Analysis of 5G network slice brokering case," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, 2018, pp. 185–190.

[152] W. Lin, X. Xu, L. Qi, X. Zhang, W. Dou, and M. R. Khosravi, "A proof-of-majority consensus protocol for blockchain-enabled collaboration infrastructure of 5G network slice brokers," in *Proc. 2nd ACM Int. Symp. Blockchain Secure Crit. Infrastruct.*, 2020, pp. 41–52.

[153] K. Papadakis-Vlachopapadopoulos, I. Dimolitsas, D. Dechouniotis, E. E. Tsiropoulou, I. Roussaki, and S. Papavassiliou, "Blockchain-based slice orchestration for enabling cross-slice communication at the network edge," in *Proc. IEEE 20th Int. Conf. Softw. Qual. Rel. Security Companion (QRS-C)*, 2020, pp. 140–147.

[154] K. Papadakis-Vlachopapadopoulos, I. Dimolitsas, D. Dechouniotis, E. E. Tsiropoulou, I. Roussaki, and S. Papavassiliou, "On blockchain-based cross-service communication and resource orchestration on edge clouds," *Informatics*, vol. 8, no. 1, p. 13, 2021.

[155] P. Gorla, V. Chamola, V. Hassija, and D. Niyato, "Network slicing for 5G with UE state based allocation and blockchain approach," *IEEE Netw.*, vol. 35, no. 3, pp. 184–190, May/Jun. 2021.

[156] S. B. Saad, A. Ksentini, and B. Brik, "A trust architecture for the SLA management in 5G networks," in *Proc. ICC*, 2021, pp. 1–6.

[157] P. Alemany et al., "Transport network slices with security service level agreements," in *Proc. 22nd Int. Conf. Transp. Opt. Netw. (ICTON)*, 2020, pp. 1–4.

[158] R. Vilalta et al., "Applying security service level agreements in V2X network slices," in *Proc. IEEE Conf. Netw. Funct. Virtualizat. Softw. Defined Netw. (NFV-SDN)*, 2020, pp. 114–115.

[159] "INSPIRE-5Gplus." Accessed: Jun. 16, 2021. [Online]. Available: https://www.inspire-5gplus.eu/

[160] L. Suárez, D. Espes, F. Cuppens, C.-T. Phan, P. Bertin, and P. Le Parc, "Managing secure inter-slice communication in 5G network slice chains," in *Proc. IFIP Annu. Conf. Data Appl. Security Privacy*, 2020, pp. 24–41.

[161] "Network functions virtualisation (NFV) release 3; security; security management and monitoring specification disclaimer," ETSI, Sophia Antipolis, France, Rep. ETSI GS NFV-SEC 013 V3.1.1 (2017–02), 2017.

[162] J. Zhang, Y. Liu, Z. Li, and Y. Lu, "Forecast-assisted service function chain dynamic deployment for SDN/NFV-enabled cloud management systems," *IEEE Syst. J.*, vol. 17, no. 3, pp. 4371–4382, Sep. 2023.

[163] H. Wang, Y. Wu, G. Min, and W. Miao, "A graph neural network-based digital twin for network slicing management," *IEEE Trans. Ind. Informat.*, vol. 18, no. 2, pp. 1367–1376, Feb. 2022.

[164] Q. Liu, T. Han, and N. Ansari, "Learning-assisted secure end-to-end network slicing for cyber-physical systems," *IEEE Netw.*, vol. 34, no. 3, pp. 37–43, May/Jun. 2020.

[165] A. H. Celdrán, M. G. Pérez, F. J. G. Clemente, F. Ippoliti, and G. M. Perez, "Policy-based network slicing management for future mobile communications," in *Proc. 5th Int. Conf. Softw. Defined Syst. (SDS)*, 2018, pp. 153–159.

[166] I. Afolabi, A. Ksentini, M. Bagaa, T. Taleb, M. Corici, and A. Nakao, "Towards 5G network slicing over multiple-domains," *IEICE Trans. Commun.*, vol. 100, no. 11, pp. 1992–2006, 2017.

[167] P. Schneider, C. Mannweiler, and S. Kerboeuf, "Providing strong 5G mobile network slice isolation for highly sensitive third-party services," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2018, pp. 1–6.

[168] J. B. B. Abdo, H. Chaouchi, and M. Aoude, "Ensured confidentiality authentication and key agreement protocol for EPS," in *Proc. Symp. Broadband Netw. Fast Internet (RELABIRA)*, 2012, pp. 73–77.

[169] V. N. Sathi, M. Srinivasan, P. K. Thiruvasagam, and S. R. M. Chebiyyam, "A novel protocol for securing network slice component association and slice isolation in 5G networks," in *Proc. 21st ACM Int. Conf. Model. Anal. Simulat. Wireless Mobile Syst.*, 2018, pp. 249–253.

[170] D. Sattar and A. Matrawy, "Optimal slice allocation in 5G core networks," *IEEE Netw. Lett.*, vol. 1, no. 2, pp. 48–51, Jun. 2019.

[171] B. Brik and A. Ksentini, "On predicting service-oriented network slices performances in 5G: A federated learning approach," in *Proc. IEEE 45th Conf. Local Comput. Netw. (LCN)*, 2020, pp. 164–171.

[172] A. Boubendir, F. Guillemin, S. Kerboeuf, B. Orlandi, F. Faucheux, and J.-L. Lafragette, "Network slice life-cycle management towards automation," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM)*, 2019, pp. 709–711.

[173] X. Li, C. Guo, L. Gupta, and R. Jain, "Efficient and secure 5G core network slice provisioning based on VIKOR approach," *IEEE Access*, vol. 7, pp. 150517–150529, 2019.

[174] W. da Silva Coelho, A. Benhamiche, N. Perrot, and S. Secci, "On the impact of novel function mappings, sharing policies, and split settings in network slice design," in *Proc. 16th Int. Conf. Netw. Service Manag. (CNSM)*, 2020, pp. 1–9.

[175] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.

[176] M. Ammar, G. Russello, and B. Crispo, "Internet of things: A survey on the security of IoT frameworks," *J. Inf. Security Appl.*, vol. 38, pp. 8–27, Feb. 2018.

[177] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[178] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[179] P. Ranaweera, V. N. Imrith, M. Liyanag, and A. D. Jurcut, "Security as a service platform leveraging multi-access edge computing infrastructure provisions," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2020, pp. 1–6.

[180] "What is security as a service? A definition of secaas, benefits, examples, and more." Dec. 2018. [Online]. Available: https://digitalguardian.com/blog/what-security-service-definition-secaas-benefits-examples-and-more

[181] Y. Khettab, M. Bagaa, D. L. C. Dutra, T. Taleb, and N. Toumi, "Virtual security as a service for 5G verticals," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2018, pp. 1–6.

[182] G. Blanc, N. Kheir, D. Ayed, V. Lefebvre, E. M. de Oca, and P. Bisson, "Towards a 5G security architecture: Articulating software-defined security and security as a service," in *Proc. 13th Int. Conf. Availabil. Rel. Security*, 2018, pp. 1–8.

[183] V. A. Cunha, D. Corujo, J. P. Barraca, and R. L. Aguiar, "MTD to set network slice security as a KPI," *Internet Technol. Lett.*, vol. 3, no. 6, 2020, Art. no. e190.

[184] P. Ahokangas et al., "Business models for local 5G micro operators," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 3, pp. 730–740, Sep. 2019.

[185] Y. Siriwardhana, P. Porambage, M. Ylianttila, and M. Liyanage, "Performance analysis of local 5G operator architectures for Industrial Internet," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11559–11575, Dec. 2020.

[186] S. Khan, J. Abdullah, N. Khan, A. Julahi, and S. Tarmizi, "Quantum-elliptic curve cryptography for multihop communication in 5G networks," *Int. J. Comput. Sci. Netw. Security*, vol. 17, no. 5, pp. 357–365, 2017.

[187] R. Nejabati et al., "First demonstration of quantum-secured, inter-domain 5G service orchestration and on-demand NFV chaining over flexi-WDM optical networks," in *Proc. Opt. Fiber Commun. Conf.*, 2019, p. Th4C–6.

[188] R. Wang et al., "End-to-end quantum secured inter-domain 5G service orchestration over dynamically switched flex-grid optical networks enabled by a q-ROADM," *J. Lightw. Technol.*, vol. 38, no. 1, pp. 139–149, Jan. 2020.

[189] R. S. Tessinari et al., "Field trial of dynamic DV-QKD networking in the SDN-controlled fully-meshed optical metro network of the bristol city 5GUK test network," in *Proc. 45th Eur. Conf. Opt. Commun. (ECOC)*, 2019, pp. 1–4.

[190] A. Aguado et al., "Quantum technologies in support for 5G services: Ordered proof-of-transit," in *Proc. 45th Eur. Conf. Opt. Commun. (ECOC)*, 2019, pp. 1–3.

[191] P. Wright et al., "5G network slicing with QKD and quantum-safe security," *J. Opt. Commun. Netw.*, vol. 13, no. 3, pp. 33–40, 2021.

[192] M. S. Siddiqui et al., "Policy based virtualised security architecture for SDN/NFV enabled 5G access networks," in *Proc. IEEE Conf. Netw. Funct. Virtualizat. Softw. Defined Netw. (NFV-SDN)*, 2016, pp. 44–49.

[193] A. Hermosilla, A. M. Zarca, J. B. Bernabe, J. Ortiz, and A. Skarmeta, "Security orchestration and enforcement in NFV/SDN-aware UAV deployments," *IEEE Access*, vol. 8, pp. 131779–131795, 2020.

[194] M. A. Togou et al., "A distributed blockchain-based broker for efficient resource provisioning in 5G networks," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, 2020, pp. 1485–1490.

[195] M.-W. Shih, S. Lee, T. Kim, and M. Peinado, "T-SGX: Eradicating controlled-channel attacks against enclave programs," in *Proc. NDSS*, 2017. [Online]. Available: https://www.ndss-symposium.org/ndss2017/accepted-papers/

[196] A. Banchs, G. de Veciana, V. Sciancalepore, and X. Costa-Perez, "Resource allocation for network slicing in mobile networks," *IEEE Access*, vol. 8, pp. 214696–214706, 2020.

[197] J. P. D. B. Gonçalves, H. C. De Resende, E. Municio, R. Villaça, and J. M. Marquez-Barja, "Securing E-health networks by applying network slicing and blockchain techniques," in *Proc. IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2021, pp. 1–2.

[198] B. Niu, W. You, H. Tang, and X. Wang, "5G network slice security trust degree calculation model," in *Proc. 3rd IEEE Int. Conf. Comput. Commun. (ICCC)*, 2017, pp. 1150–1157.

[199] V. N. Sathi, M. Srinivasan, P. K. Thiruvasagam, and S. R. Murthy, "Novel protocols to mitigate network slice topology learning attacks and protect privacy of users' service access behavior in softwarized 5G networks," *IEEE Trans. Depend. Secure Comput.*, vol. 18, no. 6, pp. 2888–2906, Nov./Dec. 2021.

[200] H. Wang, Y. Wu, G. Min, J. Xu, and P. Tang, "Data-driven dynamic resource scheduling for network slicing: A deep reinforcement learning approach," *Inf. Sci.*, vol. 498, pp. 106–116, Sep. 2019.

[201] S. D'Oro, F. Restuccia, T. Melodia, and S. Palazzo, "Low-complexity distributed radio access network slicing: Algorithms and experimental results," *IEEE/ACM Trans. Netw.*, vol. 26, no. 6, pp. 2815–2828, Dec. 2018.

[202] Q. Hu, W. Wang, X. Bai, S. Jin, and T. Jiang, "Blockchain enabled federated slicing for 5G networks with AI accelerated optimization," *IEEE Netw.*, vol. 34, no. 6, pp. 46–52, Nov./Dec. 2020.

[203] S. Parvin, A. Gawanmeh, S. Venkatraman, A. Alwadi, J. N. Al-Karaki, and P. D. Yoo, "A trust-based authentication framework for security of WPAN using network slicing," *Int. J. Elect. Comput. Eng.*, vol. 11, no. 2, p. 1375, 2021.

[204] J. Ortiz et al., "INSPIRE-5Gplus: Intelligent security and pervasive trust for 5G and beyond networks," in *Proc. 15th Int. Conf. Availabil. Rel. Security*, 2020, pp. 1–10.

Chamitha De Alwis (Senior Member, IEEE) received the B.Sc. degree (First Class Hons.) in electronic and telecommunication engineering from the University of Moratuwa, Sri Lanka, in 2009, and the Ph.D. degree in electronic engineering from the University of Surrey, U.K., in 2014. He is a Lecturer with the School of Computer Science and Technology, University of Bedfordshire, U.K. He is the Founder Head of the Department of Electrical and Electronic Engineering, University of Sri Jayewardenepura, Sri Lanka, where he also worked as a Senior Lecturer. He too has worked in the capacity of a consultant and a network engineer in the telecommunication industry. He is research active and has a proven track record of publications. He was awarded several competitive grants, while he has also actively contributed to many research projects, including EU FP7 funded research projects. His main research interests are network security, 5G/6G, and blockchain.

Pawani Porambage (Senior Member, IEEE) received the B.Sc. degree from the University of Moratuwa, Sri Lanka, in 2010, the M.Sc. degree from the University of Nice Sophia-Anipolis, France, in 2012, and the Doctoral degree in communications engineering from the University of Oulu, Finland, in 2018. She is a Senior Researcher with the VTT Technical Research Centre of Finland. She is also a Docent with the University of Oulu, where she was a Researcher with the Centre for Wireless Communication from 2012 to 2022. Her main research interests include lightweight security protocols, 6G security, blockchain, security and privacy on IoT and MEC, network slicing, and wireless sensor networks.

Kapal Dev (Senior Member, IEEE) received the Ph.D. degree from the Politecnico di Milano, Italy, in 2019, under the Prestigious Fellowship of Erasmus Mundus funded by the European Commission. He is currently working as an Assistant Lecturer with the Department of Computer Science, Munster Technological University, Ireland. He is also working as a Senior Research Associate with Lebanese American University, Lebanon, and the Institute for Intelligent Systems, University of Johannesburg, South Africa. He is an expert external evaluator of most prestigious European Research Council starting grant, several MSCA Co-Fund schemes, Elsevier, IET, Springer Book proposals, and top scientific journals and conferences. He is very active in leading successful projects as a Principal Investigator under Horizon Europe MSCA Staff Exchange, Erasmus + International Credit Mobility, Capacity Building for Higher Education, and H2020 CO-FUND projects and won over 1.2 million Euros funding in total. He has published over 70 plus research papers majorly in top IEEE transactions, magazines, and conferences. His research interests include wireless communication networks, blockchain, and artificial intelligence targeting applications majorly towards industry 4.0/5.0 and supervised more than 22 students at masters and Ph.D. level in the same areas. He is recently award as IEEE ComSoc EMEA Outstanding Young Researcher 2022 for promising research activities for the benefit of the Society. He received the Tom Brazil Excellence in Research Award from SFI Funded CONNECT Research Centre. He received 2022 Irish Research Council Research Ally Prize for his mentoring/supervison services. He has also received the IEEE ComSoc Excellent Reviewer Award from IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING in 2022. He recently delivered invited talk on "Unlocking the Future: Exploring the Enchanting Possibilities of 6G" under IEEE ComSoc Distinguish Speaker Program at MUET, Jamshoro, Pakistan. He is serving as a Funded Investigator at one of top European research centres– CONNECT, Trinity College Dublin funded by Science Foundation. He is serving as an Associate Editor for *IEEE Consumer Electronics Magazine*, *Nature*, *Scientific Reports*, *Wireless Networks* (Springer), *IET Quantum Communication*, and *IET Networks*, an Area Editor for *Physical Communication* (Elsevier), and a Technical Committee Member in Elsevier COMCOM. He is a Professional Member of ACM.

Thippa Reddy Gadekallu (Senior Member, IEEE) received the bachelors's degree in computer science and engineering from Nagarjuna University, India, the Master of Technology degree in computer science and engineering from Anna University, Chennai, India, and the Ph.D. degree from the Vellore Institute of Technology, Vellore, India. He is currently working as a Chief Engineer with Zhongda Group, Jiaxing, Haiyan, China, as well as an Associate Professor with the School of Information Technology and Engineering, Vellore Institute of Technology. He is also working as an Adjunct Professor with Lebanese American University, Lebanon, Jiaxing University, China, and Lovely Professional University, India. He has more than 14 years of experience in teaching. He has published more than 200 papers in reputed journals/conferences. His research areas include machine learning, the Internet of Things, deep neural networks, blockchain, and computer vision. He is an Academic Editor in journals, such as *PLOS One*, Nature (Springer), and *Expert Systems* (Wiley). He is also serving as a Reviewer in many journals, such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE ACCESS, IEEE INTERNET OF THINGS JOURNAL, IEEE SOFTWARE, *IEEE Consumer Electronic Magazine*, *Soft Computing*, *Applied Soft Computing*, *Future Generation Computer Systems*, *Multimedia Tools and Applications*, *Journal of Ambient Intelligence and Humanized Computing*, *Transactions on Emerging Telecommunications Technologies* (Wiley), *Internet Technology Letters* (Wiley), *Ah HoC Networks*, *Sustainable Computing: Informatics and Systems*, *Computer Networks*, and *Computer Communications*. He was recently recognized as one of the top 2% scientists in the world as per Elsevier's survey in 2021 and 2022.

Madhusanka Liyanage (Senior Member, IEEE) received the Doctor of Technology degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. He is an Assistant Professor/Ad Astra Fellow and the Director of Graduate Research with the School of Computer Science, University College Dublin, Ireland. He is leading the Network Softwarization and Security Labs, UCD School of Computer Science, which mainly focuses on the security and privacy of future mobile networks, including 5G and 6G. He is also acting as an Adjunct Professor with the University of Oulu, the University of Ruhuna, Sri Lanka, and the University of Sri Jayawardhanepura, Sri Lanka. He has secured over five Million euros in research funding via various research projects. His research interests are 5G/6G, blockchain, network security, artificial intelligence, explainable AI, federated learning, network slicing, Internet of Things, and multi-access edge computing. He also received the prestigious Marie Skłodowska-Curie Actions Individual Fellowship and the Government of Ireland Postdoctoral Fellowship from 2018 to 2020. In 2020, he received the "2020 IEEE ComSoc Outstanding Young Researcher" Award from IEEE ComSoc EMEA. Also, he was awarded an Irish Research Council Research Ally Prize as part of the IRC Researcher of the Year 2021 awards for his positive impact as a Supervisor. In 2022, he received "The 2022 Tom Brazil Excellence in Research Award" from the SFI CONNECT Center. He is a PI for three large EU H2020/Horizon Europe projects on 6G and AI security. Two research projects (MEVICO and SIGMONA Projects) received the CELTIC Excellence and CELTIC Innovation Awards in 2013, 2017, and 2018. He is also an Expert Consultant at the European Union Agency for Cybersecurity. Moreover, he is an expert reviewer at different funding agencies in France, Qatar, UAE, Sri Lanka, and Kazakhstan. In 2021 and 2022, he was ranked among the World's Top 2% Scientists (2020 and 2021) in the List that Elsevier BV, Stanford University, USA prepared. For more information, see www.madhusanka.com.