Journal of Network and Computer Applications 214 (2023) 103621

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

Open RAN security: Challenges and opportunities

Madhusanka Liyanage [a,*], An Braeken [b], Shahriar Shahabuddin [c,d], Pasika Ranaweera [a]

[a] School of Computer Science, University College Dublin, Ireland
[b] Department of engineering, technology (INDI), Vrije Universiteit Brussel, Belgium
[c] Mobile Networks, Nokia, Dallas, TX, USA
[d] Centre for Wireless Communications, University of Oulu, Finland

ARTICLE INFO

Keywords:
Open RAN
Security
Privacy
O-RAN
5G
6G
AI
Machine learning
Virtualization
Radio access network

ABSTRACT

Open RAN (ORAN, O-RAN) represents a novel industry-level standard for RAN (Radio Access Network), which defines interfaces that support inter-operation between vendors' equipment and offer network flexibility at a lower cost. Open RAN integrates the benefits and advancements of network softwarization and Artificial Intelligence to enhance the operation of RAN devices and operations. Open RAN offers new possibilities so different stakeholders can develop the RAN solution in this open ecosystem. However, the benefits of Open RAN bring new security and privacy challenges. As Open RAN offers an entirely different RAN configuration than what exists today, it could lead to severe security and privacy issues if mismanaged, and stakeholders are understandably taking a cautious approach towards the security of Open RAN deployment. In particular, this paper analyzes the security and privacy risks and challenges associated with Open RAN architecture. Then, it discusses possible security and privacy solutions to secure Open RAN architecture and presents relevant security standardization efforts relevant to Open RAN security. Finally, we discuss how Open RAN can be used to deploy more advanced security and privacy solutions in 5G and beyond RAN.

1. Introduction

Mobile network communications are becoming one of the critical enablers of the current digital economy and interconnecting national critical infrastructure-based services (Berkeley et al., 2010). The number of mobile subscribers and different mobile-based services is increasing rapidly all across the globe (O'Dea, 2021). However, the radio spectrum is still scarce, and optimal utilization of radio resources is critical for developing a telecommunication network (Faulhaber and Farber, 2003). Thus, the orchestration and management of radio resources or the Radio Access Network (RAN) also evolved with each mobile generation. The early mobile generation mobile network architectures, such as 2G and 3G, had controllers responsible for the orchestration and management of RAN and its resources (Gindraux, 2002). The flat network architecture in 4G enables a new interface (i.e., X2) to support base station level communication to handle RAN resource allocation (Dahlman et al., 2013). However, the RAN of existing mobile network generations is still based on monolithic building blocks. Thus, RAN functions of existing networks, including most of the 5G network, are still contained with the proprietary vendor-specific devices called Baseband Units (BBUs) at the base stations (Parvez et al., 2018). However, this approach leads to the proverbial vendor lock-in RAN since different RAN vendors can design their flavor of RAN equipment. This has eliminated the possibility for MNOs (Mobile Network Operators) to get mix-and-match services from other RAN vendors.

The introduction of the network softwarization concept in 5G (Nguyen et al., 2021; Condoluci and Mahmoodi, 2018; Yang et al., 2013) and added intelligence in beyond 5G networks have opened up a promising solution, called Open RAN, to mitigate this issue (Yang et al., 2013; Gavrilovska et al., 2020). The Open RAN Alliance (Umesh and Teshima, 2020) went back to the controller concept to enable best-of-breed Open RAN. Open Radio Access Networks (Open RANs), also known as ORANs or O-RANs, have been considered one of the most exciting RAN concepts designed for 5G and beyond wireless systems. Open RAN promotes openness and added intelligence for RAN network elements that could overcome the limitations of existing RAN technologies, Niknam et al. (2020) and Bonati et al. (2022). The feature of openness allows smaller and new players in the RAN market to deploy their customized services, while the feature of intelligence is to increase automation and performance by optimizing the RAN elements and network resources. Moreover, Open RAN offers many RAN solutions and elements to the network operators to be more open

* Corresponding author.
E-mail addresses: madhusanka@ucd.ie (M. Liyanage), an.braeken@vub.be (A. Braeken), shahriar.shahabuddin@nokia.com (S. Shahabuddin), pasika.ranaweera@ucd.ie (P. Ranaweera).

https://doi.org/10.1016/j.jnca.2023.103621
Received 12 April 2022; Received in revised form 15 August 2022; Accepted 6 March 2023
Available online 21 March 2023

Summary of Important Acronyms

3GPP	3rd Generation Partnership Project
AI	Artificial Intelligence
API	Application Programming Interface
CA	Certificate Authority
CICA	Canadian Institute of Chartered Accountants
CN	Container
COTS	Commercial Off-The-Shelf
(D)DoS	(Distributed) Denial of Service
DU	Distributed Unit
eCPRI	Enhanced Common Public Radio Interface
ETSI	European Telecommunications Standards Institute
FRANS	Fair, Reasonable and Non-Discriminatory
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
IPSec	Internet Protocol Security
LTE-M	Long-Term Evolution for Machines
MIMO	Multiple Input Multiple Output
ML	Machine Learning
MTBF	Mean Time Between Failures
NF	Network Function
NVD	National Vulnerability Database
O-Cloud	Open Cloud
O-DU	Open Distributed Unit
Open RAN	Open Radio Access Network
OS	Operating System
PBCH	Physical Broadcast Channel
PNF	Physical Network Function
RAM	Random Access Memory
rApp	non-real-time Intelligence Application
RRM	Radio Resource Management
RU	Radio Unit
SI	System Integration
S Plane	Synchronization Plane
SUPI	Subscription Permanent Identifier
SQL	Structured Query Language
TPM	Trusted Platform Module
UE	User Equipment
U Plane, UP	User plane
VIP	Very Important Person
VNF	Virtual Network Function
xApp	near-real-time intelligence Application
5G	Fifth Generation
AICPA	American Institute of Certified Public Accountants
BBU	Baseband Unit
CIA	Confidentiality, Integrity, Availability
CI/CD	Continuous Integration / Continuous Delivery
CNF	Containerized or Cloud-Native Network Function
CPU	Central Processing Unit
DL	Downlink
E2E	End-to-end
EI	Election Infrastructure
FH	Fronthaul
FTP	File Transfer Protocol
gNB	Next generation NodeB
GUTI	Global Unique Temporary Identifier
HW	Hardware
IP	Intellectual Property
JTAG	Joint Test Action Group
MI	Model Inversion
MITM	Man In The Middle
M-Plane	Management Plane
Near-RT	Near-Real-Time
Non-RT	Non-Real-Time
OAM	Operations, Administration and Maintenance
O-CU	Open Centralized Unit
OFH	Open Fronthaul
O-RU	Open RAN Radio Unit
OSS	Operations Support Systems
PDCCH	Physical Downlink Control Channel
PTP	Precision Time Protocol
RAN	Radio Access Network
RIC	Radio Access Network Intelligent Controller
RRU	Remote Radio Unit
SSH	Secure Shell
SMO	Service Management and Orchestration
SRM	Supplier Relationship Management
SW	Software
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UL	Uplink
vCU	Virtual Computational Unit
VM	Virtual Machine
vRAN	virtualized Radio Access Network

and flexible. Further, the network operators can shorten the time-to-market of new applications and services to maximize the overall revenue because of the virtualization feature. Thus, the added intelligence in Open RAN could offer superior benefits even to existing network softwarization-based virtual RAN and cloud RAN concepts.

There are two major Open RAN organizations, i.e., Telecom Infra Project (TIP) (TIP, 2022) and the O-RAN alliance (RAN, 2022) who are working on the advancement of Open RAN realization. The TIP's OpenRAN program is an initiative that focuses on developing solutions for future RANs based on disaggregation of multi-vendor hardware, open interfaces, and software. O-RAN Alliance is another Open RAN organization that mainly focuses on defining and enforcing new standards for Open RAN to ensure interoperability among the different vendors. At the beginning of 2020, a liaison agreement between TIP and O-RAN was made to ensure their alignment in developing interoperable Open RAN solutions. OpenRAN development of TIP has a similar original goal similar to O-RAN. Thus, we use the term "Open RAN" throughout the paper regarding both OpenRAN and O-RAN development efforts.

O-RAN refers to the O-RAN Alliance or designated specification.

However, the benefits of Open RAN come with challenges, e.g., security, deterministic latency, and real-time control (Singh et al., 2020; Gavrilovska et al., 2020; Polese et al., 2022). Among these factors, the security in Open RAN is quite essential. As 5G and beyond networks are responsible for interconnecting many Internet protocol Telephony

(IpT) based critical national infrastructure, attacks on future telecommunication networks will have a ripple effect (Mantas et al., 2015; Batalla et al., 2020). Some devastating examples caused by such attacks are smart cities and factories shutting down, a complete black-out of the power grids and water supplies, a fall-out of the transportation infrastructure with crashes by autonomous vehicles, etc. Soldani (2019) and Ahmad et al. (2018). These challenges demand significant effort from the research and industry communities to standardize and implement security for all 5G and beyond sections, including Open RAN networks (Tataria et al., 2021). Especially the decentralization of control functions with Open RAN increases the number of threat vectors and the surface area for attacks.

Open RAN has distinct features that bring intelligence to future networks. While AI helps overcome various challenges of 6G Open RANs via intelligent and data-driven solutions, it can hurt the security of RAN. Attackers can target AI systems or even use AI-based attacks to jeopardize the operation of the Open RAN system. Thus, Open RAN will now be vulnerable to AI-related attacks such as denial-of-service (DoS) (Needham, 1993), spoofing (van der Merwe et al., 2018), and malicious data injection (Illiano and Lupu, 2015) could affect the AI. For instance, AI training can be manipulated in an Open RAN spectrum access system by inserting fake signals. In addition, the integration of network softwarization will add a whole new set of security attacks related to virtualization. Similar to the 5G core and edge networks, now Open RAN needs to tackle softwarization-associated attacks such as Virtual Network Function)/Cloud Network Function (VNF/CNF) manipulation (Kawashima, 2021), Virtual Machine (VM) misconfiguration (Jarraya et al., 2015), log leak attacks (Wright et al., 2003). In addition, open interfaces defined in Open RAN will introduce another security and privacy vulnerability set. Thus, it is necessary to develop correct security and privacy solutions to mitigate these new Open RAN-related security and privacy solutions at the radio network level. Existing security mechanisms, frameworks, and governance approaches will need to be upgraded to operate in an open multi-vendor controlled Ecosystem.

On the other hand, added features of Open RAN can bring security and privacy advantages over traditional RAN. Open RAN can also build upon the security enhancements already enabled by 5G and allow the operator to control the network's security entirely, ultimately enhancing the operational security of their network. Less hardware dependency and support for complete software control in Open RAN allow isolating security breaches quickly and intelligently, reducing the impact of security risk. In addition, these features reduce the risks associated with security mechanism upgrades. Moreover, the modularity supported by the open interface in Open RAN allows the security and privacy deployments to support continuous integration/continuous delivery (CI/CD) operating model (Bobrovskis and Jurenoks, 2018). The CI/CD model supports seamless and effective security management against the security vulnerability in Open RAN.

Moreover, Open RAN enables the possibility for zero-touch and frequent software updates (Dutta et al., 2021), which is more transparent, fast, secure, and low-cost than the software upgrades in a traditional network. Finally, standardization of open interfaces can also reduce security risks to a certain extent as it can help detect incongruencies and offer concrete steps to monitor the network. Thus, it is crucial to identify these new security benefits and rectify them correctly in future RAN deployments.

1.1. Motivation

The research on Open RAN security is still in its infancy. As Open RAN advocates open interfaces, it is imperative to analyze the security vulnerabilities and their mitigation of Open RAN in parallel to their system architecture development. The reason is that without a proper security framework in place, the idea of an open network might not be an attractive solution to the network operators. This is especially true in this era of complex geopolitics, where global powers are increasingly concerned about wireless infrastructure security. Table 1 summarizes existing research works about Open RAN security. The table highlights the lack of a comprehensive Open RAN security analysis in the literature. Most existing Open RAN-related publications focused on architecture, interfaces, and algorithms, while security was a secondary topic. A couple of technical specifications from the Open RAN alliance present the security flaws and solutions of Open RAN in O-Ran Alliance Security Focus Group (2021a), and O-Ran Alliance Security Focus Group (2021b), respectively. However, they are not comprehensive because they lack a thorough discussion either on the solutions or the flaws. They also do not present the Open RAN security benefits or discuss any research directions. Similarly, other publications presented in Table 1 fail to provide a comprehensive analysis of Open RAN security.

1.2. Our contribution

To the best of the authors' knowledge, this is the first attempt to provide a comprehensive security analysis of Open RAN. The main contributions of this article are presented below.

- **Classification of security-related risks**: A taxonomy distinguishing the risks present in Open RAN, is provided. Each of these risks is elaborated concerning a description of impact.
- **Present Open RAN specific security solutions**: Unique solutions for Open RAN security vulnerabilities based on blockchain, physical layer, and AI have been presented.
- **Overview of general mistakes, consequences, and mitigation**: A summary of the general design errors pertaining to Open RAN, their consequences, and potential mitigation are presented.
- **Discussion on Open RAN security benefits**: A list of security benefits specific to Open RAN, and already available in V-RAN and 5G networks are presented.

1.3. Outline

The rest of the paper is organized as follows. Section 2 presents the overview of Open RAN architecture and the difference from the conventional RAN architectures. The threat vectors and security risks associated with Open RAN are presented in Section 3. Several solutions for the security threats and vulnerabilities of Open RAN are elaborated in Section 4. Section 5 presents the security benefits of Open RAN implementation. Discussion and lessons learned towards realizing an Open RAN architecture is portrayed in Section 6. Finally, Section 7 concludes the paper.

2. Brief overview of Open RAN architecture

Unlike traditional RAN technology, Open RAN decouples hardware and software bonds in proprietary RAN equipment. This feature offers more flexibility for mobile operators to deploy and upgrade their RAN segment (Yang et al., 2013; Niknam et al., 2020; Johnson et al., 2022). Fig. 1 illustrated the key differences between traditional and Open RAN architectures.

The Open RAN architecture is proposed to enable three main goals (Garcia-Saavedra and Costa-Perez, 2021; Gavrilovska et al., 2020), i.e.;

- Cloudification: The goal is to support cloud-native RAN functions via disaggregated hardware and software components.
- Intelligence and automation: The goal is to utilize advanced AI/ML capabilities to enable automated management and orchestration in RAN
- Open internal RAN interfaces: The goal is to support various Open RAN interfaces, including interfaces defined by 3GPP.

Table 1
Summary of publications relevant to Open RAN security.

Year & Ref.	Open RAN architecture	Open RAN security flaws	Open RAN security solutions	Open RAN security benefits	Research directions	Remarks
2022 (Wypiór et al., 2022)	H	L	L	L	L	A review article on RAN evolution towards open models and potential Open RAN benefits and market trends
2022 (Masur et al., 2022)	M	L	L	L	L	This article discusses Open RAN deployment with a focus on 5G network device security
2021 (Altiostar, 2021)	H	M	H	L	L	A whitepaper by Altiostar on the security of Open RAN which presents a method to implement Open RAN with a zero-trust security framework
2021 (Garcia-Saavedra and Costa-Perez, 2021)	H	L	L	L	L	An article that summarizes Open RAN specifications focusing on proposed architecture and building blocks
2021 (Dryjański et al., 2021)	H	L	L	L	L	This article presents an analysis of an Open RAN system with the aid of a traffic steering use case implemented in a modular way
2021 (O-Ran Alliance Security Focus Group, 2021a)	H	H	L	L	L	A technical specification by O-RAN alliance on Open RAN security threat modeling and remediation analysis
2021 (Abdalla et al., 2021)	H	H	L	M	L	A pre-print which identifies the limitations of current Open RAN architecture and the technologies and opportunities for research and development to overcome them
2021 (O-Ran Alliance Security Focus Group, 2021b)	M	M	H	L	L	A technical specification by O-RAN alliance on the security requirements and security controls per Open RAN defined interface and Open RAN defined network function
2021 (Dik and Berger, 2021)	M	L	M	L	L	Presented an analysis to demonstrate the urgent need to protect Open RAN fronthaul and proposed a security protocol as a potential solution
2020 (Ericsson, 2020)	L	M	L	L	L	A whitepaper by Ericsson on Open RAN security considerations that ensure an open and interoperable RAN is secure by design
2020 (Gavrilovska et al., 2020)	H	L	L	L	L	This article presents the basic functionalities and current research trends on C-RAN and its derivatives such as vRAN and Open RAN
2017 (Tian et al., 2017)	L	M	M	L	L	A survey of C-RAN security flaws and solutions where many threats and solutions are relevant for Open RAN.
This Paper	H	H	H	H	H	A comprehensive security analysis of Open RAN which thoroughly discusses the Open RAN security architecture, security flaws and solutions and security benefits of Open RAN

H — High Coverage: Consider the factor in reasonable or high detail.

M — Medium Coverage: Partially considers the factor (leaves out vital aspects or discusses it in relation to other factors).

L — Low Coverage: Did not Consider the factor or only very briefly discussed it through mentioning it in passing.

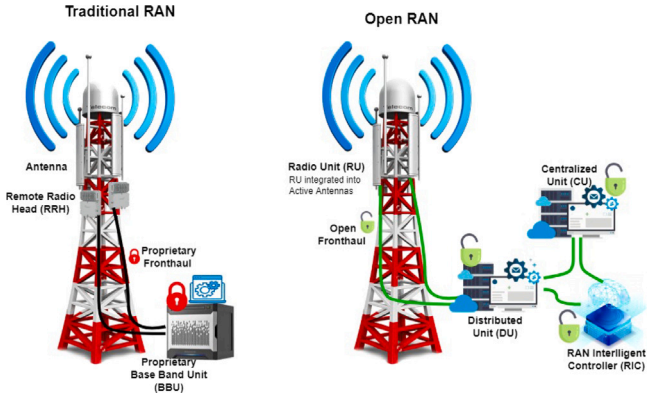

Fig. 1. High-level comparison of Open RAN with traditional RAN.

As illustrated in Fig. 1, the RAN in Open RAN architecture is disaggregated into four main building blocks, i.e., the Radio Unit (RU), the Distributed Unit (DU), the Centralized Unit (CU), and RAN Intelligence Controller (RIC). The RU is located with antennas, and it is responsible for transmitting, receiving, amplifying, and digitizing radio frequency signals. The former BBU (Based Band Unit) is now disaggregated into DU and CU. They are the computation parts of the base station. Here, DU is physically located closer to RU, while CU can be located closer to the Core. RIC is possible for taking intelligent and automated decisions related to RAN.

O-RAN appliance has proposed a more detailed architecture for Open RAN as represented in Fig. 2. The main elements of the Open RAN architecture include Service Management and Orchestration (SMO), RAN Intelligence Control (RIC), O-Cloud, Open RAN central unit (O-CU), Open RAN distributed unit (O-DU), and Open RAN radio unit (O-RU).

- **Service Management and Orchestration (SMO)**: The SMO framework is a core component of the Open RAN architecture, whose main responsibility is to manage the RAN domain, such as the provision of interfaces with network functions, near-real-time RIC for RAN optimization, and O-Cloud computing resource and workload management (Wang et al., 2021; Wypiór et al., 2022). These SMO services can be performed through four interfaces, including A1, O1, O2, and open fronthaul M-plane.
- **RAN Intelligence Control (RIC)**: This logical function enables Open RAN to perform real-time optimization of functions and resources through data collected from the network and end-users. It is the key element in Open RAN, which helps to realize disaggregation strategy, bringing multivendor interoperability, intelligence, agility, and programmability to RANs (Balasubramanian et al., 2021; Masur et al., 2022). The RIC is divided into components non-real-time RIC (Non-RT RIC) and near-real-time RIC (Near-RT RIC). The Non-RT RIC is integrated with Open RAN SMO Framework. It handles the control request and RAN resources within the second range. To this task, Non-RT RIC utilizes specialized applications called rApps. Non-RT RIC can also collect network performance metrics and subscriber data to

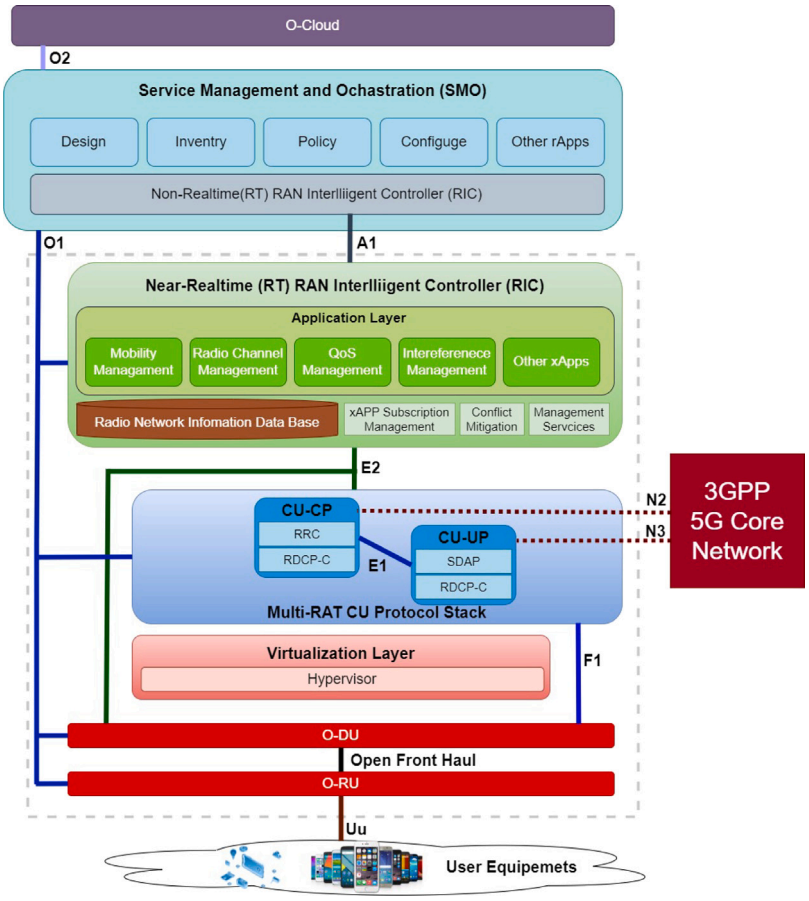

Fig. 2. The high-level architecture of Open RAN proposed by the O-RAN alliance.

offer AI-based network optimization and policy guidance recommendations for Near-RT RIC. The Near-RT RIC resides within edge servers or regional clouds as it is responsible for performing network optimization actions within the milliseconds range. Near-RT RIC uses the different xApps to support these tasks (Orhan et al., 2021; Dryjański et al., 2021).

- **O-Cloud**: This is a physical computing platform. It creates and hosts the various virtual network functions (VNFs) and cloud network functions (CNFs) which are used by near-real-time RIC, O-CU control plane, O-CU user plane, and O-DU (Tamim et al., 2021).
- **O-DU**: This logical node has functionalities of the physical and MAC layers. This element terminates the E2 with F1 interfaces.
- **O-CU**: This is a logical node in the Open RAN architecture and hosts all the functions of both the control plane and data plane. These two O-CU planes connect with the O-DU logical node via the F1-c interface and F1-u interface, respectively.
- **O-RU**: This logical node has a physical layer and radio signal processing capabilities to connect with the SMO framework via the open fronthaul M-plane interface and connects with end-users via radio interfaces.

One of the main goals of Open RAN is "opening" the protocols and interfaces between these RAN components, such as radios, hardware, and software. The O-RAN Alliance has defined eleven different interfaces, including A1, O1, E1, F1 open fronthaul M-plane, and O2. More specifically, the open fronthaul M-plane interface is to connect Service Management and Orchestration Framework (SMO) and Open RAN radio unit (O-RU), and A1 is to connect non-real-time RAN intelligent controller (RIC) located in the SMO framework and near real-time RIC for RAN optimization, O1 is to support all Open RAN network functions when they are connected with SMO, and O2 is to connect SMO and O-Cloud for providing cloud computing resource and workflow management. According to Garcia-Saavedra and Costa-Perez (2021), there are different deployment scenarios of the O1 interface, such as flat, hierarchical, and hybrid models, by which the SMO framework can provide numerous management services, for example, provisioning management services, trace management services, and performance management services.

3. Threat vectors and security risks associated with Open RAN

We start by explaining the taxonomy, used to distinguish the different types of risks. Next, each of the four identified domains is further elaborated.

3.1. Threat taxonomy

We categorize the risks into three main domains: Process, Technology, and Global. First, process risks are related to rules, regulations, and oversight. Second, the technology risks correspond with the risks caused by the mechanisms for enforcing rules and procedures, as well as detecting threats. Third, global risks are broad risks related to global communication instruction. Fig. 3 provides an overview of the risk domains in Open RAN respectively.

3.2. Process

In the process risks, four categories are distinguished, corresponding to the preliminary assumptions or prerequisites, the general regulations, the privacy, and human-related aspects. In fact, all the process

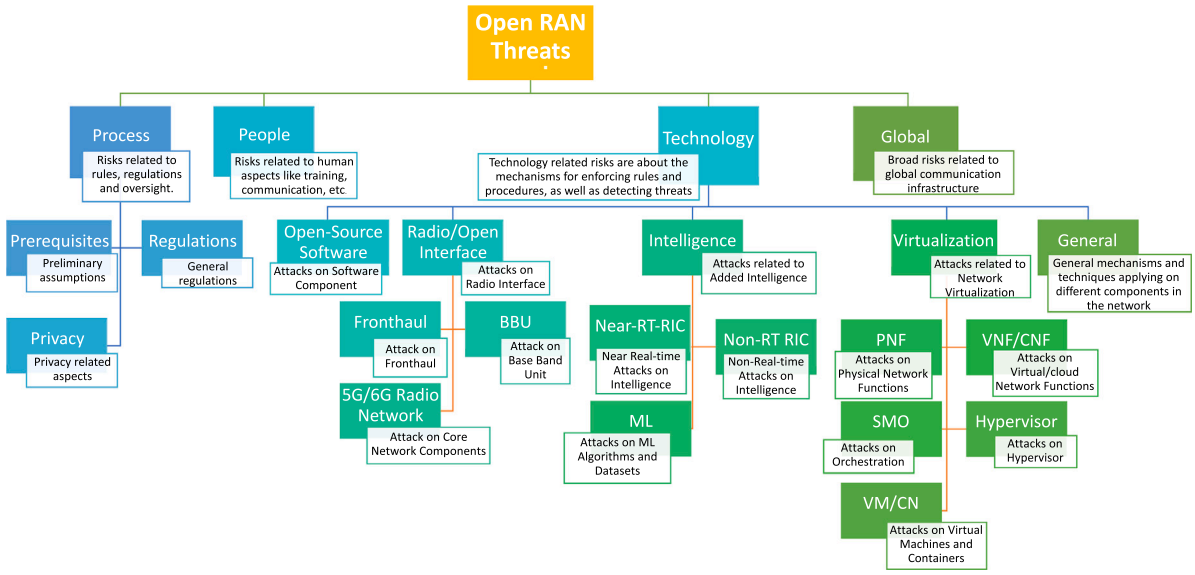

Fig. 3. The threat taxonomy of Open RAN systems.

risks apply to any RAN implementation but are in general more complex in Open RAN due to the modularity and the higher amount of stakeholders involved. Table 2 provides an overview of the key process risks associated with the Open RAN process.

3.2.1. Prerequisites

To operate a successful Open RAN system, a list of minimum prerequisites and assumptions of the operational environment needs to be defined. However, The prerequisites are not under the control of the RAN system but should be carefully checked (Ziegler and Yrjölä, 2021). To start with, a reliable operational environment must be ensured, providing for instance reliable timestamps to be used in the audit records (Palmbach and Breitinger, 2020; O-Ran Policy Coalition, 2021).

Next, secure storage of stored logs, credentials, and secrets in external systems needs to be guaranteed for instance by using hardware-based security modules like trusted platform modules (TPMs) (Sevinç et al., 2007; O-Ran Policy Coalition, 2021). Cryptographic key management, remote attestation, disk image encryption, and secure booting are functions that are typically conducted by a TPM. O-RAN requires such an entity within its midst for managing hardware-based security and a root of trust for facilitating signing and verification functions.

In addition, access to this sensitive data should only be allowed by privileged users (O-Ran Policy Coalition, 2021). The last prerequisite is that the certificate authorities (CAs), which authenticate the network elements, are fully trusted and audited by well-established, worldwide recognized organizations (O-Ran Policy Coalition, 2021; Dong et al., 2016). In fact, all these prerequisites are essential for any RAN implementation. However, since there are more stakeholders involved in Open RAN, it is clear that these requirements are more challenging to enforce and verify, compared to other RAN implementations.

3.2.2. General regulations

The first step in the effective Open RAN launch that needs to be done is the standardization of critical processes like operation, administration, and management, covering the complete lifecycle of the Open RAN deployment (Kawahara and Matsukawa, 2019). This includes a clear description of components used for the secure establishment of mutual authentication, access control, key management, trusted communication, storage, boot and self-configuration, update, recoverability and backup, security management of risks in open source components, security assurance, privacy, continuous security development, testing, logging, monitoring and vulnerability handling, robust isolation, physical security, cloud computing and virtualization, and robustness.

Next, it is also important to identify, locate, authenticate, and verify the origin of the relevant assets in the system. Furthermore, for each of the different assets, at rest and in transit and location, the type (data, component, etc.) and the security properties (Confidentiality, Integrity, Availability — CIA) should be carefully collected. In fact, a complete and efficient supply chain process is required (Hassija et al., 2020). In particular, this is more complex for Open RAN due to the decoupling of hardware and software and the modularity. For instance, there is a risk of firms from allied states purchasing relabeled products or components from adversarial states.

Finally, when an issue arises in the network, due to the complexity of the network it is not evident to identify and isolate the issues. Moreover, in case the issue is found, it is possible that the corresponding vendors do not take their responsibility as they can pass the blame to others because of the complexity and interdependence of the whole system.

3.2.3. Privacy

The privacy of end users encompasses privacy related to data, identity, and personal information (Sorensen et al., 2015). Privacy-sensitive data for end users are mostly leaked via communication services that are gathering all types of personal information, which are often not needed for the functioning of the services. Adversaries can even further extract more personal information about end users, such as User Equipment (UE) priority, location information, trajectory, and preference. The protection of the user data is regulated by the law of the hosting country, where different jurisdictions can be applied. There are, at least, three possible locations, the victim, the offender, or the service provider (Liyanage et al., 2018). Therefore, clear guidelines should be developed in order to cope with these new interfaces, shared environments, and new players available in Open RAN.

3.2.4. People

First of all, it is necessary to clearly identify and authenticate the stakeholders involved in the different processes like implementation, management, operation, and maintenance of the Open RAN system. For each of the stakeholders, their roles and responsibilities should be clearly defined and assessed. Vendors should have well-established and transparent security practices built into their engineering processes (O-Ran Policy Coalition, 2021).

Table 2
Overview of process-related Open RAN risks.

Risk category	Threat	Description	Specific to Open-RAN
Prerequisite	Requirement of reliable operational environment	The operational environment of the Open RAN system must provide reliable timestamps for, e.g. the generation of audit records. In addition, the list of minimum prerequisites and assumptions, required to successfully operate the O-RAN system, needs to be defined for the operational environment (O-Ran Policy Coalition, 2021; Singh et al., 2020).	This is applicable to any RAN implementation. However, it is more complex in Open RAN since some aspects (e.g. cloud services) are not under the control of the Open RAN system.
	Requirement of secure storage of stored logs, credentials, and secrets	Log files, secrets, and credentials stored in external systems and related to Open RAN needs to be protected, and access control should be enabled to allow only privileged users (O-Ran Policy Coalition, 2021; Altiostar, 2021).	This is applicable to any RAN implementation. However, Open RAN hardware should possess a hardware-based security module like TPM (Trusted Platform Module) to manage, generate, and securely store cryptographic keys, to offer a secure boot, full disk encryption, and remote attestation.
	Requirement of Trusted certificate authorities (CAs)	Trusted certificate authorities for identity provisioning are applied (O-Ran Policy Coalition, 2021; Altiostar, 2021).	This is applicable to any RAN implementation. However, due to the involvement of additional stakeholders, the CAs used in Open RAN for authenticating network elements should be properly audited by well-established global organizations and SDOs
General	Requirement of Secure complete lifecycle process and assessment strategy	Network operators should have an appropriate security process for the complete lifecycle of Open RAN deployment (O-Ran Policy Coalition, 2021; Docomo, 2021).	This is applicable to any RAN implementation. However, it is more complex in Open RAN due to the involvement of additional stakeholders.
	Requirement of Trusted assets/supply chain verification	There is a need to identify, locate, authenticate, and verify the origin of the relevant assets in the Open RAN system (O-Ran Policy Coalition, 2021).	This is applicable to any RAN implementation. However, it is more complex in Open RAN because an Open RAN system is built with components coming from different additional parties.
	Increased complexity and inter-dependency	Increased difficulty in identifying issues exists and accountability due to complexity is not evident (Johnson, 2020).	This is specific to Open RAN. Due to the modularity of O-RAN and loss of total ownership. Multiple stakeholders need to collaborate to mitigate the threats
Privacy	Violation of privacy policies such as GDPR	Privacy issues arise due to new interfaces, shared environments, and new players with different views and objectives on privacy (O-Ran Policy Coalition, 2021; Liyanage et al., 2018).	Privacy issues arising from 5G C-RAN are already identified. However, the attack surface increases in the case of Open RAN as components can be designed in different regions.
People	Requirement of Trustworthy and qualified insiders	There is a need to provide sufficient security resources and sufficient security education and training for the users (O-Ran Policy Coalition, 2021; Eric Wenger, 2020; Lee-Makiyama, 2020).	The availability of sufficient security-educated people is a well-known problem. In the case of Open RAN additional expertise is required such as virtualized component security
	Requirement of Trusted stakeholders	All stakeholders involved with the Open RAN System should be identified, authenticated, and trusted (O-Ran Policy Coalition, 2021; Eric Wenger, 2020).	This is applicable to any RAN implementation. However, it is more complex in Open RAN due to the increased and diversified number of stakeholders.

Moreover, adequate training and assessments need to be organized for the different stakeholders, going from administrators, integrators, operators, and orchestrators in order to be capable of securely implementing and managing the system according to the instructions provided by the Open RAN Alliance and the later to be developed standards (O-Ran Policy Coalition, 2021).

Finally, strategies for security testing with published well-known test plans at trusted lab facilities should be defined upfront and integrated into the regular operation (O-Ran Policy Coalition, 2021) Moreover, adequate training and assessments need to be organized.

3.3. Technology

The largest class of risks is related to the different components and mechanisms in the network. Here, the distinction is made based on Docomo (2021), considering aspects related to open software, radio/open interface, intelligence, virtualization, and general. Fig. 4 provides an overview of the main technology-related risks in Open RAN.

3.3.1. Open source software

The open source related risks are well-known problems available in open-source software code. An overview is provided in Table 3. Since Open RAN is expected to be built (solely or partly) based on such open-source codes, it is, in particular, vulnerable to this type of attack.

A trusted developer can intentionally insert a backdoor by injecting a few lines of malicious code into an open-source code component to be used within the Open RAN system (Li et al., 2022). It is then highly likely that a software project team picks it up and uses the infected open source code later, while the tools for vetting and testing of the development team do not detect the malicious code (O-Ran Policy Coalition, 2021). As a consequence, a vulnerability in the software code is included and can go undetected for a long period. The resulting

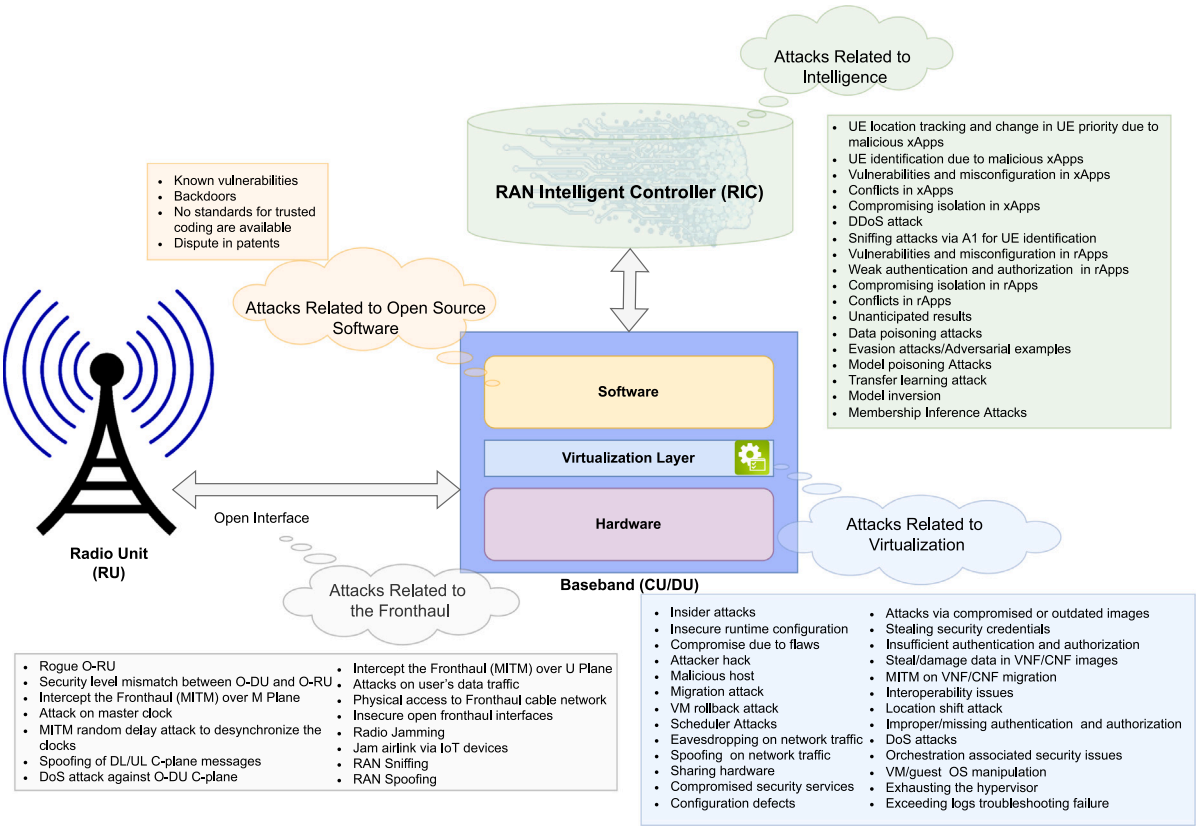

Fig. 4. A summary of related attacks on Open RAN architecture and its components.

Table 3
Overview of Open source software related Open RAN risks.

Impacting Open RAN Component	Threat	Description	Specific to Open-RAN
All	Known vulnerabilities	Attention should be paid to developers using SW components with known vulnerabilities or untrusted libraries and without proper management of interdependencies and patch management (O-Ran Policy Coalition, 2021; Carlson, 2021).	This is a well-known problem in open-source software code. Since Open RAN is expected to be built (solely or partly) based on such open source codes, it is, in particular, vulnerable to these attacks
	Backdoors	Attention should be paid to a trusted developer intentionally inserting a backdoor into an open source code Open RAN component (O-Ran Policy Coalition, 2021; Balding, 2021).	This is a well-known problem in open-source software code. Since Open RAN is expected to be built (solely or partly) based on such open source codes, it is, in particular, vulnerable to these attacks
	No standards for trusted coding available	Explicit legislative standards, guidance, requirements, or conditions to ensure trusted programming should become available (O-Ran Policy Coalition, 2021; Balding, 2021; Carlson, 2021).	This is a well-known problem in open-source software code. Since Open RAN is expected to be built (solely or partly) based on such open source codes, it is, in particular, vulnerable to these attacks
	Dispute in patents	The actors involved in Open RAN development implement 5G functions at their discretion and under different copyright regimes. The establishment of a certain type of collaboration is required between those actors as the degree of their collaboration is not at the same level in many cases (Balding, 2021; Mitchell, 2021).	Due to the need for inherent agreements in the O-RAN alliance (With the increased number of stakeholders), this is a threat specific to Open RAN.

effect on the Open RAN system can be diverse. It can either be simply annoying, but at the same time, it can significantly decrease the system performance via, for instance, Denial of Service (DoS) attacks, or it can even lead to serious loss of sensitive data.

Open source vulnerabilities are normally published on the National Vulnerability Database (NVD) (Booth et al., 2013). This database is primarily intended for developers to disclose vulnerabilities. However, this source is also used by hackers to exploit those vulnerabilities enabling backdoors to attacks on e.g., the hypervisor, Operating System (OS), Virtual Machine (VM), or container. Moreover, vulnerabilities frequently propagate as developers often re-use free open-source code. As a consequence, downloading open source libraries and their dependencies, as well as downloading open source code from untrusted repositories, contain significant risks (O-Ran Policy Coalition, 2021). Open RAN vendors and operators should thus store at each moment up-to-date inventories containing the dependencies in their open-source software used in the applications. In addition, this should be complemented by a process that receives and manages all the notifications coming from the open-source community that is related to newly discovered

vulnerabilities, including newly developed patches to overcome them. This should enable better supply chain traceability.

Existing legislation demonstrates implied security preferences but provides no explicit legislative standards, guidance, requirements, or conditions. These preferences should be explicit but transparent, reviewable, and auditable to ensure secure coding. Due to the fact a material amount of Open RAN code is being written by firms in different countries, security audits should be mandatory, making code available to security researchers (Balding, 2021).

Finally, the last open source software risk is more linked to political and financial interests instead of security interests. Both the 3GPP and Open RAN alliance operate a Fair, Reasonable, and Non-Discriminatory (FRANS) policy when it comes to patents that are held by contributors to those respective organizations. Patents are held on aspects of the 3GPP and Open RAN Alliance specifications, but the holders of those patents agree that it is mutually beneficial for everyone if the patents are licensed with an FRANS approach. The concern in this area is politically oriented. There might be a possibility that the patents held by competing manufacturers and service providers may be withdrawn from the FRANS licensing arrangement if trade relations between different countries dramatically deteriorate (Balding, 2021; Mariniello, 2011).

3.3.2. Radio/open interface

The different radio/open interface components include the Fronthaul, the central Unit/distributed unit (CU/DU), and the 5G radio network. Table 4 summarizes the threats related to this radio/open interface.

- **Fronthaul**. The Fronthaul of Open RAN, consisting of O1, O2, A1, and E2 are the new components, all available with open interfaces allowing the software programmability of RAN. These components and interfaces may not be secured to industry best practices, for instance containing no proper authentication and authorization processes, ciphering and integrity checks, protection against replay attacks, prevention of key reuse, validation of inputs, response to error conditions, etc. (O-Ran Policy Coalition, 2021). This often follows from the strict performance requirements (bandwidth, latency, fronthaul transport link length, etc.) that limit the use of some security features, enforced by the high bit rate fronthaul interface to increase the processing delay. As a consequence, different MITM, DoS, data tampering or even information disclosure attacks become possible.

  - The first category of risks is due to attacks from the internet exploiting weak authentication and access control to penetrate the network boundary. There are several possibilities for this.
    First, it would allow the presence of a rogue Open RAN Radio Unit (O-RU) in order to fool the O-DU or UE into associating with it instead of the legitimate O-RUs (O-Ran Policy Coalition, 2021). This opens the door to subscriber's identity interception/disclosure and unauthorized user tracking attacks of user movements and activities by catching the SUPI/5G-GUTI of the subscriber's User Equipment (UE) and location of a device).
    Second, an adversary can inject DL/UL C-plane messages that falsely claim to be from the associated O-DU, which would impact the O-RU to process the corresponding U-Plane packets (Amy Zwarico et al., 2020). Also spoofing of DL/UL C-plane messages, leading to temporarily limited cell performance (or even DoS) on cells served by the O-RU, and in addition, a consequential threat to all O-RUs parented to that O-DU might exist.
    Third, if, in addition, no trusted stakeholders are guaranteed, an attacker can attack a master clock by sending an excessive amount of time protocol packets or impersonate a legitimate clock, a slave, or an intermediate clock, by sending malicious messages to the master, thus degrading the victim's performance (Dik and Berger, 2021). The attacker may be residing either within the attacked network (insider) or on an external network connected to the attacked network. This attack results in a situation where the clock service is interrupted completely or the timing protocol are operational, but slaves are being provided inaccurate timing information due to the degraded performance of the master clock. This degradation in the accuracy of time may cause DoS to applications on all the RUs that rely on accurate time, potentially bringing down the cell. A cell outage caused by misaligned time may further impact performance in neighboring connected cells.
    Finally, when having two different vendors, the O-RU and the O-DU need to be managed as different entities and may have heterogeneous security levels (Ericsson, 2020). Instead, the O-DU will have to bridge the management traffic between the management system and the O-RU. Hence the possibility of reaching the northbound systems beyond the O-DU through the Open Fronthaul interface becomes a possible attack vector in this split architecture.
  - The second category of risks on the fronthaul is due to the ability of the attacker to compromise Open RAN data integrity, confidentiality, and traceability in case the components are not secured to the industry best practices. This often follows from the strict performance requirements (bandwidth, latency, fronthaul transport link length, etc.) that limit the use of some security features, enforced by the high bit rate fronthaul interface to increase the processing delay. As a consequence, different MITM attacks become possible. A MITM attacker over the fronthaul interface is able to intercept the data over the U-Plane and introduce random packet delay on the Precision Timing Protocol (PTP) sync messages and/or PTP delay-request/response messages, which causes inaccurate PTP to offset calculation, resulting in clocks which may not be synchronized properly (Dik and Berger, 2021). Also, denial of service (DoS) attacks become possible. Moreover, after breaking the PDCP security, also access to content can be obtained.
    A Man-in-the-Middle (MITM) attack over the fronthaul interface or O1 is able to intercept the M plane, and thus also to do passive wiretapping and DoS, but needs to break M Plane Security prior to gaining OAM access (O-Ran Policy Coalition, 2021).
  - The third category of risks on the fronthaul is if an attacker compromises the Open RAN monitoring mechanisms and integrity and availability of the log files (Sasaki et al., 2020).
  - The fourth category of risks on the fronthaul is caused by a compromise of the integrity and availability of the Open RAN components in general. Insufficient assurance of Open RAN software package integrity could affect CIA of data, services, hardware and policies during installation or upgrade phases for Open RAN components (O-Ran Policy Coalition, 2021). An attacker could, in such a case, cause denial-of-service, data tampering, information disclosure, spoofing identity, etc.
  - Finally, if an attacker is able to get physical access to the fronthaul components, it can result in a devastating impact on the confidentiality and integrity of the data (Bitsikas and Pöpper, 2021). Note that this is typically linked to the first type of process-related threats dealing with trusted stakeholders.

Table 4
Overview of Radio/Open Interface related Open RAN risks.

Impacting Open RAN Component	Threat	Description	Specific to Open-RAN
Fronthaul	Rogue O-RU	The idea is to fool O-DU or UE into associating it to a rogue O-RU over the legitimate O-RUs (O-Ran Policy Coalition, 2021).	It is possible to set up a rogue RU in other RAN systems as well. However, it will be easier to develop a rogue O-RU in O-RAN due to its open nature. No implicit security due to lack of know-how.
	Security level mismatch between O-DU and O-RU	An attacker penetrates O-DU and beyond through O-RU or the Fronthaul interface due to heterogeneous security levels in the split architecture (O-Ran Policy Coalition, 2021; Ericsson, 2020).	Yes, This happens only in O-RAN as different vendor equipment is possible for O-RU and O-DU.
	Intercept the Fronthaul (MITM) over M Plane	The high bit rate Fronthaul interface imposes strict performance requirements which force to limit the use of some security features (O-Ran Policy Coalition, 2021).	Yes, This interface is specific in O-RAN.
	Attack on the master clock	An attacker can attack a master clock by sending an enormous amount of time protocol packets. It can also impersonate a legitimate clock, a slave, or an intermediate clock, by sending malicious messages to the master, thus degrading the victim's performance (O-Ran Policy Coalition, 2021; Dik and Berger, 2021).	No, however, there is an increased range of attacks in Open RAN due to the use of various xApps and rApps. Moreover, the near-RT operation is expected in Open RAN for some of the functions.
	MITM random delay attack to desynchronize the clocks	An attacker acting as MITM can introduce random packet delay on Precision Timing Protocol (PTP) sync messages and/or PTP delay-req/resp messages, which causes inaccurate PTP to offset calculation, thus the clocks may not be synchronized properly (O-Ran Policy Coalition, 2021; Dik and Berger, 2021).	No, however, there is an increased range of attack in O-RAN.
	Spoofing of DL/UL C-plane messages	An adversary injects DL/UL C-plane messages that falsely claim to be from the associated O-DU which would impact the O-RU to process the corresponding U-Plane packets (O-Ran Policy Coalition, 2021; Amy Zwarico et al., 2020). This will lead to temporarily limited cell performance (or even DoS) on cells served by the O-RU and, in addition, a consequential threat to all O-RUs parented to that O-DU might exist.	No. However, there is an increased range of attacks in Open RAN. Moreover, this attack can be easier to perform in a shared virtualized environment.
	DoS attack against O-DU C-plane	DoS attacks against the O-DU C-plane is launched. O-Ran Policy Coalition (2021). Due to the cleartext nature of Enhanced Common Public Radio Interface (eCPRI) messages used for the Open Fronthaul C-Plane, an attacker can launch a volumetric DoS attack with bad or unauthenticated eCPRI Real-time control data messages (adopted for C-Plane communication) against the O-DU C-Plane, causing O-DU performance degradation and potentially its overall service interruption, which could further cascade to all its serving O-RUs.	No, however, there is an increased range of attacks in Open RAN. The openness in the Open RAN system will be a cause loss of explicit security due to a lack of know-how.
	Intercept the Fronthaul (MITM) over U Plane	An attacker attempts to intercept the Fronthaul (MITM) over the User Plane due to the limited use of some security features at the Fronthaul interfaces (O-Ran Policy Coalition, 2021).	No, This is a problem also in 3GPP RAN.
	Attacks on user's data traffic	Integrity protection is enabled on the Control Plane messages, which still makes the data traffic of the user vulnerable because the Control Plane and User Plane are segregated (O-Ran Policy Coalition, 2021; Ericsson, 2020).	No, This is a problem also in 3GPP RAN. However, Open RAN offers the computing resources (i.e. not available in other RANs) to implement 3GPP-specified UP integrity protection algorithms without impacting on the user experience.
	Physical access to Fronthaul cable network	An intruder into the exchange over the Fronthaul cable network attempts to gain electronic access to cause damage or access sensitive data (O-Ran Policy Coalition, 2021; Bitsikas and Pöpper, 2021).	The same type of attack can be applied in other RAN. However, the attack range and possibilities are increased in O-RAN.
	Insecure open Fronthaul interfaces	An attacker penetrates and compromises the O-RAN system through the open O-RAN's Fronthaul due to the lack of industry-level security best practices (O-Ran Policy Coalition, 2021; Amy Zwarico et al., 2020; Nolle, 2020).	Yes since this involves the new interfaces introduced specifically in O-RAN. Although following Nolle (2020), it is also inherently required for a secure 5G implementation.

(*continued on next page*)

Table 4 (*continued*).

Impacting Open RAN Component	Threat	Description	Specific to Open-RAN
CU/DU	Attacks via Shared Baseband Units	An attacker exploits the lack of isolation on Shared Baseband Units and the edge platforms to perform attacks (Niknam et al., 2020; Ranaweera et al., 2021).	The same type of attack can be applied in V-RAN. However, the attack range and possibilities are increased in O-RAN.
5G Radio Network	Radio jamming	An attacker could disrupt the communication by deliberately jamming, blocking, or creating interference with the authorized wireless network. O-Ran Policy Coalition (2021)	No, this is a general attack that can be applied to any RAN.
	Jam air-link via IoT devices	An attacker attempts to jam the air-link signal through IoT devices (O-Ran Policy Coalition, 2021).	No, this is applicable to any RAN.
	RAN sniffing	An attacker could decode the essential network configuration details by sniffing the RAN (O-Ran Policy Coalition, 2021).	No, this is a general attack that can be applied to any RAN.
	RAN spoofing	An attacker is spoofing the RAN signals by transmitting a fake signal meant to pretend as an actual signal (O-Ran Policy Coalition, 2021).	No, this is a general attack that can be applied to any RAN.

- **CU/DU**. The shared units pool in the Open RAN cloud native deployment may suffer from insufficient isolation and impose the risk of breaking user privacy and accessing sensitive data (Niknam et al., 2020). The openness and exposure of the CU and DU entities in comparison to C-RAN are inviting intruders to gain access to those entities through cyber hacking attempts. As the fronthaul of the O-RAN is expected to be deployed via enhanced Common Public Radio Interface (eCPRI), converged packet-based network that contrives it is inviting cyber threats unlike the traditional fronthauls (Kazemifard and Shah-Mansouri, 2021). Although uncommon, intrusions can be perpetrated via the F interface in the Mid-haul that connects CU to its corresponding DUs. Such interventions are possible through the threat vectors such as service migration, offloading, or handover mechanisms that exist with edge computing base stations that are presumed to host CUs (Ranaweera et al., 2021). A compromised CU is capable of impregnating both the fronthaul and backhaul directions leveraging the open interfaces of the O-RAN.
- **5G Radio Network**. These attacks are classical attacks, which can be applied to any RAN system and include radio jamming, jamming via IoT devices, RAN sniffing, and spoofing (O-Ran Policy Coalition, 2021).
  Radio jamming can be impacting on the reference signals, the synchronization signal, the Physical Broadcast Channel (PBCH), the Physical Downlink Control Channel (PDCD), the Physical Uplink Control Channel, or the Physical Random-Access Channel (Chi et al., 2020). This would enable an attacker to disrupt the communication by deliberately jamming, blocking, or creating interference with the authorized wireless network. Additionally to blocking the communication flow, jamming the synchronization channels or the signaling flow is another method to disrupt the 5G services (Varga et al., 2022). A capable adversary can target different entities of the 5G communication network simultaneously to impact an interference significant enough to subdue the communication. Thus, a jamming detection mechanism is mandatory to filter out the jamming frequencies in this era of 5G and beyond (Wang et al., 2022).
  In addition, due to the millions of IoT devices in the network, jamming of the air-link signals through the IoT devices can easily overload the Open RAN resources by means of Distributed DoS (DDoS) attempts carried via a botnet army of millions to billions of infected devices, on which a malware instructs to reboot all devices in a specific or targeted 5G coverage area at the same time (Wood and Stankovic, 2004). Most IoT-based services are Location Based Services (LBSs) and expect locational awareness with utmost availability. The attackers capable of jamming the GPS receiver will succeed in subduing the service to an inaccurate state (Varga et al., 2022). Since the O-RAN interfaces should be open to a common standardization to avoid vendor-specific nature, adversaries have the ability to assimilate the firmware and software specifications and induce a race-like condition by exploiting its vulnerabilities.
  RAN sniffing allows the attacker to decode essential network configuration details, assisting attackers in optimizing and crafting their attacks (Alina and Saraswat, 2021). Vulnerabilities of the PBCH channel are allowing the attackers to sniff the 5G RAN network stats (He et al., 2018). The open-source and low-cost natures of the software radio are inviting the attackers to exploit the existing vulnerabilities in software, protocol, and firmware layers. With RAN spoofing, a fake signal pretending to be an actual signal is conveyed by targeting an RF receiver within the RAN (Alina and Saraswat, 2021). Similar to sniffing, vulnerabilities of the PBCH channel and the software radio devices can be the main causes targeted through spoofing attempts that embrace the masquerading signal as a legitimate one (Lichtman et al., 2018).

3.3.3. Intelligence

The different components and mechanisms that contribute to the intelligence in the Open RAN network are the Near Realtime Radio Access Network Intelligence Controller (Near-RT-RIC), Non real-time RIC (Non-RT RIC), and machine learning (ML) algorithms. These risks are mostly specific to Open RAN as they operate on new components and new algorithms, which are currently not available. The threats related to intelligence are summarized in Table 5.

- **Near-RT-RIC related Attacks:** xApps have the capability to manipulate the behavior of a certain cell, a group of UEs, and a specific UE. The related attacks are due to either malicious xApps, xApps with vulnerabilities, misconfigured xApps, compromised xApps, or conflicting xApps (O-Ran Policy Coalition, 2021).
  As xApps are launched to perform intelligent functions for CU and DU entities in regards to radio resource management, a compromised xApp could attempt to take the control of a cell, a RU device, or a group of UE devices; and would be capable of tracking a certain consumer within its RIC domain. In addition, the same malicious xApp could gather priority information on the served UE devices through the A1 interface, where distinguishing and identifying serving UEs are possible. Such acts violate the location privacy of the important UEs and even the prioritization of the currently serving services can be manipulated. This will lead to compromise RAN performance as well as privacy violations.
  Malicious xApps can potentially be used as a sniffer for UE identification. In such a circumstance, RAN performance could

Table 5
Overview of intelligence-related Open RAN risks.

Impacting Open RAN Component	Threat	Description	Specific to Open RAN
Near-RT-RIC	UE location tracking and change in UE priority due to malicious xApps	xApps have the capability to manipulate the behavior of a certain cell, a group of UEs, and a specific UE to track a certain subscriber or change the priority level of a UE (O-Ran Policy Coalition, 2021; Ericsson, 2020).	Yes since xApps and E2, A1 interfaces are only defined in O-RAN.
	UE identification due to malicious xApps	Malicious xApps can exploit UE identification and track UE location. For example, a xApp can potentially be used as a "sniffer" for UE identification (O-Ran Policy Coalition, 2021; Ericsson, 2020; Amy Zwarico et al., 2020).	Yes since xApps and E2, A1 interfaces are only defined in O-RAN.
	Vulnerabilities and misconfiguration in xApps	Vulnerabilities can potentially exist in any xApp, if it is obtained from an untrusted or unmaintained source. An attacker exploits vulnerabilities and misconfiguration of such xAPPs to disrupt the offered network service and potentially take over another xApp or the whole near-RT RIC (O-Ran Policy Coalition, 2021; Ericsson, 2020; Abdalla et al., 2021).	Yes, as these components are only defined in O-RAN.
	Conflicts in xApps	Conflicting xApps unintentionally or maliciously impact O-RAN system functions such as mobility management, admission controls, bandwidth management, and load balancing for the purpose of performance degradation. Moreover, a threat actor can utilize a malicious xApp that intentionally triggers RRM (Radio Resource Management) decisions conflicting with the O-gNB internal decisions to create DoS (O-Ran Policy Coalition, 2021; Ericsson, 2020).	Yes, as these components are only defined in O-RAN.
	Compromising isolation in xApps	An attacker compromises xApp isolation to break out of xApp confinement. In such a way, an attacker can perform a side-channel attack to deduce information from co-hosted xApps in a shared resource pool (O-Ran Policy Coalition, 2021).	Yes, as these components are only defined in O-RAN.
Non-RT RIC	DDoS attack	An attacker penetrates the Non-Real-Time RAN Intelligent Controller (Non-RT RIC) to cause a DoS or degrade the performance (O-Ran Policy Coalition, 2021).	Yes, as these components are only defined in O-RAN.
	Sniffing attacks via A1 for UE identification	An attacker performs UE sniffing in the Non-RT RIC via the A1 interface or via the R1 interface via rApps in order to identify UE. For example, a rApp can potentially be used as a "sniffer" for UE identification (O-Ran Policy Coalition, 2021).	Yes, as these components are only defined in O-RAN.
	Vulnerabilities and misconfiguration in rApps	Vulnerabilities can potentially exist in any rApp, if it is obtained from an untrusted or unmaintained source. An attacker exploits vulnerabilities and misconfiguration of such rAPPs to disrupt the offered network service and potentially take over another rApp or the whole non-RT RIC (O-Ran Policy Coalition, 2021; Ericsson, 2020; Abdalla et al., 2021).	Yes, as these components are only defined in O-RAN.
	Weak authentication and authorization in rApps	If web front-end or REST API interfaces contain software vulnerabilities or implement authentication and authorization insufficiently, an attacker could bypasses authentication and authorization and be able to gain access to the rApp and pose as a tenant. In such a way an attacker gains the ability to manipulate configurations, access logs, and implement back doors (O-Ran Policy Coalition, 2021; Amy Zwarico et al., 2020)	Yes, as these components are only defined in O-RAN.
	Compromising isolation in rApps	An attacker compromises rApp isolation to break out of rApp confinement. In such a way, an attacker can perform a side channel attack to deduce information from co-hosted rApps in a shared resource pool (O-Ran Policy Coalition, 2021)	Yes, as these components are only defined in O-RAN.
	Conflicts in rApps	Conflicting rApps (i.e., direct, indirect, and implicit conflicts) unintentionally or maliciously impact non-realtime Open RAN system functions such as Carrier license scheduling, energy savings, and subscription handling to degrade performance or trigger a DoS (O-Ran Policy Coalition, 2021).	Yes, as these components are only defined in O-RAN.

(*continued on next page*)

be impacted negatively while the privacy of the subscribers may be violated. This follows from the fact that the A1 interface is able to point out a certain UE in the network (through its UE identifier), which creates correlations among the randomized and anonymized UE identities between the RAN nodes. As a consequence, UE location tracking and change in UE priority become possible. In particular, the identification and tracking of a certain subscriber, for instance, a Very Important Person (VIP) becomes a real threat. The exposure of the UE identifier is most probable through E2 signaling channels in comparison to its counterpart A1, due to the Near-RT conditions of the E2. Further, such malicious xApps could change the Service Level Agreement (SLA) specifications of the assigned services similar to changing the priority levels. Such acts could conflict with the Near-RT-RICs decision process as the program execution times might extend beyond the specified boundaries of a presumed Near-RT event or SLAs (Abdalla et al., 2021).

Vulnerabilities can potentially exist in any xApp since they can come from either an untrusted or unmaintained source. Such vulnerabilities can then be exploited to take over another xApp or the whole near-RT RIC and often have the purpose to degrade the performance (e.g. a DoS). It may also be possible to alter

Table 5 (*continued*).

Impacting Open RAN Component	Threat	Description	Specific to Open RAN
ML	Unanticipated results	If unexplainable AI is used, the results cannot be predicted and might have a fast impact (Yampolskiy, 2020). Therefore, the use of unexplainable AI/ML models in the Open-RAN can potentially lead to unanticipated consequences, which might have an impact on security and privacy (Amy Zwarico et al., 2020). Such AI/ML models could unintentionally violate security and privacy policies and offer biased results.	The same type of attack can be applied in V-RAN. However, the attack range and possibilities are larger in O-RAN.
	Data poisoning attacks	An attacker with access to the training set is able to poison the ML training data (Data poisoning attacks) and thus break the reliability of the training. This impacts the xApps/rApps managed Open RAN system functions such as mobility management, admission controls, bandwidth management, and load balancing and results in a performance degradation (O-Ran Policy Coalition, 2021; Sun et al., 2021).	This attack only applies to O-RAN, where ML is explicitly included.
	Evasion attacks/Adversarial examples	An attacker uses an adversarial example (intentionally designed date) as an input to the ML models to make a mistake (Siriwardhana et al., 2021; Goodfellow et al., 2017; Iturria-Rivera et al., 2022). This impacts the xApps/rApps managed Open RAN system functions resulting in performance degradation.	This attack only applies to O-RAN, where ML is explicitly included.
	Model poisoning Attacks	An attacker with access to the model can alter the ML model resulting in system manipulation and compromise of ML data confidentiality and privacy (O-Ran Policy Coalition, 2021; Iturria-Rivera et al., 2022; Shi and Sagduyu, 2021). This impacts the xApps/rApps managed Open RAN system functions resulting in performance degradation.	This attack only applies to O-RAN, where ML is explicitly included.
	Transfer learning attack	A transfer learning attack becomes possible (O-Ran Policy Coalition, 2021). This impacts the xApps/rApps managed Open RAN system functions resulting in performance degradation.	This attack only applies to O-RAN, where ML is explicitly included.
	Model inversion	An attacker can have the aim to reconstruct training data from model parameters (Siriwardhana et al., 2021; Michael Veale and Edwards, 2018; Chen et al., 2020). This impacts the xApps/rApps managed Open RAN system functions resulting in performance degradation.	This attack only applies to O-RAN, where ML is explicitly included.
	Membership Inference Attacks	An attacker tries to identify the data samples used for the model training (Siriwardhana et al., 2021; Hu et al., 2021). This impacts the xApps/rApps managed Open RAN system functions resulting in performance degradation.	This attack only applies to O-RAN, where ML is explicitly included.

data transmitted over A1 or E2 interfaces or to extract sensitive information. Also, the xApp isolation can be exploited in order to break out of the xApp confinement and to deduce information from co-hosted xApps. In addition, unauthorized access provides new opportunities to exploit vulnerabilities in other xApps or Open RAN components to intercept and spoof network traffic, and to degrade services (through DoS). The open source nature of the xApps is advertising the vulnerabilities to the adversaries while misconfigurations and incompatibilities are inevitable with the open nature of the O-RAN.

Finally, since there is no clear functional split between the Near-RT RIC and the Open RAN Next Generation Node B (O-gNB), possible conflicts, including conflicts in xApps, between the decisions taken by the Near-RT RIC and the O-gNB regarding the radio resource management can appear, both unintentionally or maliciously. This can have an impact on the Open RAN system functions such as mobility management, admission controls, bandwidth management, and load balancing, potentially resulting in performance degradation. Moreover, the isolation of xApps is critical for the independent operation of O-RAN services and for accurate Near-RT-RIC decision-making. Such isolation or confinement can be penetrated through underlying system vulnerabilities, deducing access information via shared resource applications, or masqueraded authentication attempts. A compromised isolation could subdue the xApp operations to the attacker.

- **Non-RT RIC related Attacks:** rApps impact non-RT RIC functions such as AI/ML model training, A1 policy management, enrichment information management, network configuration optimization for the purpose of performance degradation, DoS, and enrichment data sniffing (UE location, trajectory, navigation information, and GPS data). rApps bearing many resemblances to xApps in their operational context have the ability to manipulate the behavior of a certain cell, a group of UEs, and a specific UE. The related attacks are similar to xApps, due to either malicious rApps, rApps with vulnerabilities, misconfigured rApps, compromised rApps, or conflicting rAPPs. Besides these similar ones, there are two more risks identified related to Non-RT RIC (O-Ran Policy Coalition, 2021).

  Untrusted or unmaintained sources can cause vulnerabilities in any rApp. The exploitation of these vulnerabilities mostly leads to disruption of the offered network service and potentially taking over another rApp or the whole non-RT RIC. As a consequence, the attacker may gain the ability to alter data transmitted over the A1 interface or extract sensitive information. Also, rApp isolation can be exploited to break out of rApp confinement and to deduce information from co-hosted rApps. Unauthorized access provides new opportunities to exploit vulnerabilities in other rApps or Open RAN components to intercept and spoof network traffic, to degrade services through DoS attempts; An attacker might also penetrate the non-RT RIC through A1/O1 interfaces or from external sources through SMO and attempts to trigger a DoS or degrade the performance of non-RT RIC (Abdalla et al., 2021).

  In addition, rApps in the Non-RT RIC can cause conflicting decisions as they can be launched by different vendors targeting different purposes: Carrier license scheduling, or energy savings. Such conflicts could take the form of a direct, indirect, or implicit nature depending on the rApp parameters in question, and the

effect that particular conflict is inducing. Direct ones deal with the conflict of the same parameter change requested by different rApps, indirect ones where the different parameter changes by different rApps would cause an opposite effect, and implicit ones that different parameter changes would lead to changing the network state. The effects can lead to an overall network performance degradation or instabilities within the network entities. These conflicts are difficult to mitigate since dependencies are impossible to observe.

There is an additional vulnerability that can appear in the case the rApp management is exposed to a web front-end or REST API, whose software interfaces contain vulnerabilities or do not implement authentication and authorization in a proper way. This would allow an attacker to gain access to the rApp and pose as a tenant or to manipulate configurations, access logs, or to implement back doors.

- **ML related Attacks:** ML and AI play a vital role in the formation of the O-RAN concept. Thus, vulnerabilities or flows in existing ML models or algorithms can be envisaged as probable threats to the O-RAN system as they are deployed in the intelligence portion of the architecture. One of the most common threats is the data poisoning attacks, where the adversary is altering the data sets that are intended for training, testing, or validating (Sun et al., 2021; O-Ran Policy Coalition, 2021). The access to perform such modifications, however, can be gained via penetration through fronthaul, mid-haul, xApps, or rApps. Poisoning attempts could impact any stage of the ML process as in feature selection, prediction, decision-making, model classification, or anomalous detection. The O-RANs' openness and the Near-RT operations require the ML models to be formed online with continual updating during the operation. Though it would not impact in the long run, feeding bogus data to the online ML model is capable of impacting the RIC decision-making negatively, especially in terms of radio resource allocation. Similarly, evasion/ adversarial attacks or model poisoning attacks represent two variants of the poisoning attack. In the evasion attempt, data is carefully tampered with according to a perturbed design that would not detect anomalously. In the model poisoning attempt, the entire model or the control parameters of the model are altered to impact the learning phases of the process (Shi and Sagduyu, 2021).

  Pre-trained and widely available ML models can be utilized by attackers for gaining access or evading the system's anomalous detectors for launching transfer learning attacks. Model inversion and membership inference attacks are ensuing privacy leakages (Siriwardhana et al., 2021). In model inversion attempts, the adversary is reconstructing the training data set from the model parameters (Michael Veale and Edwards, 2018; Chen et al., 2020; Benzaïd and Taleb, 2020). This is plausible as there are plenty of online repositories with training data that would aid the attacker in cross-validating the determined data. Membership inference threat would determine whether a particular data set was used in the training process of the ML model or not (Hu et al., 2021). Finally, due to the complexity of the models in AI/ML, the results are not yet explainable in most of the cases (Yampolskiy, 2020). Therefore, its use in the RAN can potentially lead to unanticipated consequences, which might have an impact on the security or performance (Amy Zwarico et al., 2020).

  The impact of data poisoning attempts would clearly target the allocation and management of radio resources within the O-RAN fronthaul and could result in jeopardizing the accuracy of mobility management, load balancing, and QoS management functions that are administered under the Near-RT-RIC. In the long run, the entire RT intelligent framework could become compromised. Model poisoning, evasion, and transfer learning attempts induce the same impact on the RT systems. For the Non-RT system, however, as the time is not a critical parameter, the impact would be less costly, as the decisions are made from the data gathered from an extended period in comparison to the RT instances.

3.3.4. Virtualization

The following components, Physical Network Function (PNF), Virtual Network Function (VNF), Cloud Network Function (CNF), SMO, hypervisor, and Virtual Machine/Container (VM/CN), are involved in the virtualization process. Here, we discuss the security issues associated with each of these components. Some of these attacks can be applied also in V-RAN and C-RAN (Hossain et al., 2019). However, the attack range and impact of such attacks are larger in Open RAN. The threats related to intelligence are summarized in Table 6.

- **PNF related Attacks:**. An attacker compromises a PNF to launch reverse attacks and other attacks against VNFs/CNFs. A lack of security policies to protect mixed PNF-VNF/CNF deployments, resulting in insecure interfaces, could be exploited to perform attacks against VNFs/CNFs, potentially taking advantage of legacy security used by PNFs and not provided by the virtualization/containerization layer (O-Ran Policy Coalition, 2021). Apart from the security policies, service level agreements, and service specifications are vital consensus for the PNF, CNF, and VNF entity deployment. As these entities are envisaged to launch security management entities as specified in Benzaïd and Taleb (2020), the original consensus should not be altered for all the service level guarantees.
- **VNF/CNF related Attacks:** Despite VNF/CNF images being effectively static archive modules including all components used to run a given Open RAN VNF/CNF, modules within an image may have vulnerabilities, that introduce malware, miss critical security updates, or are outdated. These images are only collections of files packaged together. Therefore, malicious files can be included intentionally or inadvertently within them. In addition, VNF/CNF images may also have configuration defects, e.g. configuring a specific user with greater privileges than needed. This could all be used to attack other VMs/CNs or hosts within the environment. An attacker can migrate a compromised VNF/CNF to a different location that has fewer security or privacy policies to gain additional access to the system. Since Open RAN uses different equipment with different vendors and different configurations, there can be less secure environments, which can lead to additional vulnerabilities if deployed in the same system (O-Ran Policy Coalition, 2021).

  Moreover, since many Open RAN VNFs/CNFs require secrets to enable authentication, access control, and secure communication between components, these secrets are embedded directly into the image file system. In addition, the images often contain also sensitive components like an organization's proprietary software and administrator credentials. Anyone with access to the image (e.g. by means of insufficient authentication and authorization) can easily parse it to extract these secrets, resulting in the compromise, stealing, or damage of the contents of the images. As a result, it can lead to Intellectual Property (IP) loss and expose significant technical details about an Open RAN VNF/CNF image to an attacker. Even more critically, because registries of images are typically trusted as a source of valid, approved software, compromise of a registry can potentially lead to compromise of downstream VMs/CNs and hosts (O-Ran Policy Coalition, 2021). There is an increased risk of MITM attacks by intercepting network traffic intended for registries in order to steal developer or administrator credentials within that traffic. This can result in fraudulent or outdated images to orchestrators (O-Ran Policy Coalition, 2021). Further, typical VNF/CNF-based security threats exist, as in location shift attacks where the adversary is capable of displacing the VNF to a domain inheriting a lesser level of security policy assignment with the intention of gaining access, or interoperability issues between the VNF/CNF developers or service providers that can be exploited by an attacker (Lal et al., 2017; Ranaweera et al., 2021).

Table 6
Overview of virtualization-related Open RAN risks.

Impacting Component	Threat	Description	Specific to Open-RAN
PNF-VNF/CNF	Lack of security policies to protect mixed PNF-VNF/CNF	Compromises a PNF to launch reverse attacks and other attacks against VNFs/CNFs due to the lack of security policies to protect mixed PNF-VNF/CNF (O-Ran Policy Coalition, 2021; Benzaïd and Taleb, 2020).	Can be applied in V-RAN. However, the attack possibilities are increased in Open RAN.
VNF/CNF	Attacks via compromised or outdated images	Compromises VNF/CNF images or used outdated images (O-Ran Policy Coalition, 2021)	The same type of attack can be applied in V-RAN.
	Configuration defects	Utilizes the configuration defect of VNF/CNF to attack (O-Ran Policy Coalition, 2021).	However, the attack range and possibilities are increased in Open RAN.
	Stealing security credentials	Steals embedded security credentials from VNF/CNF images (O-Ran Policy Coalition, 2021).	
	Insufficient authentication and authorization	Insufficient authentication and authorization can lead to IP loss and expose significant technical details about an Open RAN VNF/CNF image to an attacker (O-Ran Policy Coalition, 2021).	
	Stealing or damage of embedded information from VNF/CNF images	Steal or damage sensitive information from/in VNF/CNF images (O-Ran Policy Coalition, 2021).	
	MITM on VNF/CNF migration	Performs MITM to intercept network traffic and jeopardize the VNF/CNF image migration (O-Ran Policy Coalition, 2021; Ranaweera et al., 2021).	
	Interoperability issues	Exploits the security level mismatches of different VNF/CNFs (Khan et al., 2020; Liyanage et al., 2018; Ranaweera et al., 2021; Lal et al., 2017).	
	Location shift attack	A compromised VNF/CNF changes the run-time environments to perform an attack (Khan et al., 2020; Lal et al., 2017; Ranaweera et al., 2021)	
SMO	Improper/missing authentication	Can exploit the improper/missing authentication on Service Management and Orchestrator (SMO) functions to illegally access the SMO and its functions (O-Ran Policy Coalition, 2021).	The same type of attack can be applied against the Management and Orchestration (EMM) in C-RAN.
	Improper/missing authorization	Can exploit the improper/missing authorization on SMO functions (O-Ran Policy Coalition, 2021).	However, the attack range and possibilities are larger in Open RAN.
	DoS attacks	Performs overload or flooding DoS attacks at SMO (O-Ran Policy Coalition, 2021).	
	Orchestration associated security issues	Exploits weak orchestrator configuration, access control and isolation (O-Ran Policy Coalition, 2021).	Can be applied in V-RAN. However, the attack possibilities are higher in Open RAN.
Hypervisor	VM/guest OS manipulation	Exploits the security weaknesses in the guest OS to attack the hypervisor (Yang and Fung, 2016; Khan et al., 2020; Ferrag et al., 2018).	The same type of attack can be applied in V-RAN.
	Exhausting the hypervisor	Changing the configurations of compromised VNFs/CNFs to consume more resources and exhaust the hypervisor (Yang and Fung, 2016; Khan et al., 2020; Ranaweera et al., 2021).	However, the attack range and possibilities are larger in Open RAN.
	Exceeding logs troubleshooting failure	Changing the configurations of compromised VNFs/CNFs to generate excessive amounts of logs and exhaust the hypervisor (Yang and Fung, 2016; Khan et al., 2020).	
	Insider attacks	An insider who has access to the hypervisor misuses his privileges to perform an attack (Yang and Fung, 2016; Khan et al., 2020).	

(*continued on next page*)

- **SMO related Attacks:** As the SMO is the key entity behind the holistic autonomic environment of the O-RAN, its security is extremely vital for the O-RAN performance and the individual subscriber security and privacy. Improper or insufficient authentication or authorization of Open RAN external (e.g. AI/ML, Emotional Intelligence (EI), Human–Machine) or internal (e.g. over O1 or O2 interfaces, with Non-RT RIC) interfaces on SMO, allow access to the SMO and in particular the data stored on it. Besides disclosing Open RAN sensitive information, the attacker may also alter the Open RAN components (O-Ran Policy Coalition, 2021). DoS attacks or increased traffic can cause overload situations and thus affects the availability of the SMO data and functions. Further, an attacker may exploit weak orchestrator configuration, access control, and isolation. A single orchestrator may run many different VMs/CNs, each managed by different teams, and with different sensitivity levels. If the access provided to users and groups is not conforming to their specific requirements, an attacker or careless user would be able to affect or subvert the operation of another VM/CN managed by the orchestrator. Malicious traffic from different VMs/CNs sharing the same virtual networks may be possible if VMs/CNs of different sensitivity levels are using the same virtual network with poor isolation of inter-VM/CN network traffic (O-Ran Policy Coalition, 2021).
- **Hypervisor related Attacks:** An attacker can exploit the security weaknesses in the guest OS to attack the hypervisor of the hosting OS. Examples of guest OS vulnerabilities are OS command injection, SQL injection, buffer overflow or missing authentication for critical functions (Yang and Fung, 2016; Khan et al., 2020; Ferrag

Table 6 (*continued*).

Impacting Component	Threat	Description	Specific to Open-RAN
VM/CN	Misuse to attack others	A VM/CN can be misused to attack another VM/CN, hypervisor/container engine, other hosts (memory, network, storage), etc. (O-Ran Policy Coalition, 2021)	The same type of attack can be applied in V-RAN.
	Insecure run-time configuration	Insecure VM/CN run-time configuration by the administrator can lower the security (O-Ran Policy Coalition, 2021).	However, the attack range and possibilities are larger in Open RAN.
	Compromise due to flaws	VMs/CNs may be compromised due to flaws in the VNFs/CNFs they run (O-Ran Policy Coalition, 2021; Tanakas et al., 2021; George et al., 2021).	
	Attacker hack	Hack into VM/CN retrieves the administrator privileges, resulting in obtaining all tenant's tokens and the administrator rights of the whole Open RAN system (O-Ran Policy Coalition, 2021).	
	Malicious host	The host OS has access to all data (Ericsson, 2020; Brandão et al., 2021).	
	Migration attack	During the VM/CN migration, a MITM attacker can modify arbitrary VM/CN OS or application states (Yang and Fung, 2016; Khan et al., 2020).	
	VM rollback attack	An attacker uses an older snapshot of VM/CN to obtain access to the system (Yang and Fung, 2016; Khan et al., 2020).	
	Scheduler Attacks	Misconfigures the hypervisor scheduler to allocate more resources to malicious VMs (Yang and Fung, 2016; Khan et al., 2020).	
	Eavesdropping on network traffic	Eavesdrop on network traffic via a malicious VM/CN or hypervisor/container engine (O-Ran Policy Coalition, 2021).	
	Spoofing on network traffic	Intercept and spoof on network traffic via VMs/CNs (O-Ran Policy Coalition, 2021).	
	Sharing Hardware	Applications may share the same hardware resources in virtualization, which might be affected by vulnerabilities (Ericsson, 2020).	
	Compromised security services	Compromises auxiliary/supporting network and security services (O-Ran Policy Coalition, 2021).	

et al., 2018). Privilege escalation is a common threat among hypervisor deployments that is also applicable in the context of the O-RAN. In this attack, any authorization violations are sought out by the perpetrator exploiting the infrastructure vulnerabilities formed through ill-maintenance or misconfigurations (Ranaweera et al., 2021). The administrative capabilities granted to the adversary through this threat are devastating as they could range from a simple excessive allocation of resources to a complete deletion of xApps or rApps (Alnaim et al., 2019; Qiang et al., 2018).

An attacker may also change the configurations of compromised VNFs/CNFs to consume high amounts of CPU, hard disk, and memory resources in order to exhaust the hypervisor. Another way to compromise the hypervisor is by generating an excessive amount of log entries such that it is infeasible or very difficult to analyze the log files coming from other VNFs (Yang and Fung, 2016; Khan et al., 2020).

Finally, as the hypervisor provides its own security functions and Application Programming Interfaces (APIs) to the host system security functions, it is in full control of the security functionalities of the lower layers and thus needs to be fully trusted. When a malicious administrator has for instance root access to the hypervisor and by using a search operation, the user identity (ID), passwords and Secure Shell Protocol (SSH) keys from the memory dump can be extracted, which in turn violates the user privacy and data confidentiality (Yang and Fung, 2016; Khan et al., 2020).

- **VM/CN related Attacks:** VMs/CNs may be compromised due to flaws in the Open RAN VNFs/CNFs they run. For example, an Open RAN VNF/CNF may be vulnerable to cross-site scripting (SQL) injection (Tanakas et al., 2021) and buffer overflow vulnerabilities (George et al., 2021).

  Insecure VM/CN runtime configuration by the administrator can lower the security of the Open RAN system. It may expose VMs/CNs and the hypervisor/container engine to increased risk from a compromised VM/CN. For example, it could be used to elevate privileges and attack VMs/CNs, the O-Cloud infrastructure/services, etc. (O-Ran Policy Coalition, 2021).

  A compromised VM/CN will be able to alter that VM/CN in order to access other VMs/CNs, monitor VM/CN to VM/CN communications, attack the O-Cloud infrastructure/services, scan the network to which it is connected to in order to find other weaknesses to be exploited, etc. The container engine (in case of CN) or hypervisor (in case of VM) has access to all RAM memory, and disk volumes mounted on the virtual machines and containers. This means that a malicious VM/CN or hypervisor/container engine can get access to all Open RAN network data processed in the workloads. An attacker can launch a noisy neighbor attack against the shared O-Cloud infrastructure to cause the Open RAN system performance degradation and/or the services disruption by depriving the resources required by various Open RAN running functions (O-Ran Policy Coalition, 2021).

  An attacker hack into VM/CN is for instance possible if an attacker steals VMs/CNs private key from one VM/CN and so reveals the administrator privileges. Next, all tenant's tokens and the administrator rights of the whole Open RAN system can be obtained, O-Ran Policy Coalition (2021).

  From the side of the application, trust is required at all levels. In case the underlying host OS is malicious, access can be obtained to all data processed in the workloads, as in RAM memory and disk volumes. Techniques like secure enclaves (Brandão et al., 2021) have the goal to provide a trusted environment. However, the application will be hardware-instance dependent (Ericsson, 2020).

  If VM/CN migration is not secured or performed over a secure channel, a MITM attacker can modify arbitrary VM/CN OS or application states during the migration. An attacker may also use an older snapshot of VM/CN without the concern of the VM/CN

Table 7
Overview of global Open RAN risks.

Threat	Description	Specific to Open-RAN
Attack on digital economy	Network communications play an important role in the digital economy of a country and can cause huge damage in case of failure (Rasser and Riikonen, 2020; Bugár et al., 2020), e.g. shutting down of smart cities, crashing of autonomous electrical vehicles or going dark of factories. In particular, special attention should be given to avoid loss of trust with the users in case of such attacks as they might endanger the entire growth of the network (Spremić and Šimunic, 2018).	These threats are very general and in particular related to attacks against the communication infrastructure. There are independent of the usage of Open RAN.
Espionage	Network communications can be abused to enable espionage (Rasser and Riikonen, 2020; Bederna and Szadeczky, 2020) and there are currently no regulations for allowing or avoiding collaborations among different suppliers or actors in the network. Without being sure of the good intentions of each of the involved entities offering the equipment and software in the network, espionage at all levels, from the government to corporate, might be possible. As a consequence, it is extremely important that proper global ethical restraints are formulated on a global scale.	These threats are very general and in particular related to attacks against the communication infrastructure. There are independent of the usage of Open RAN. However, the use of SW makes Open RAN more vulnerable than RAN
Attacks on critical infrastructure	Network communications play an important role in the operation, management, and maintenance of critical infrastructures (Rasser and Riikonen, 2020), like power grids, water supplies, manufacturing, and transportation. Since the control of this infrastructure is handed over to the network operators, their responsibilities are of ultimate importance within the O-RAN domain.	These threats are very general and in particular related to attacks against the communication infrastructure. There are independent of the usage of Open RAN.
Violence against democracy	Besides espionage to dedicated people, also every other citizen can be envisaged (Rasser and Riikonen, 2020). This might be a real threat to democracy or freedom of speech in the world and it should thus be avoided in any case that one actor receives full control.	These threats are very general and in particular related to attacks against the communication infrastructure. There are independent of the usage of Open RAN.
Majority attacks and supply chain concerns	It is a danger if there is a significant involvement in Open RAN development from one country or one region, facilitating possibilities for Braeke (2020) and Balding (2021) any type of attack. Special attention should be given that no new secret alliances are formed, and therefore a well-balanced spread among the suppliers of O-RAN equipment and software is required.	These threats are very general and in particular related to attacks against the communication infrastructure. There are independent of the usage of Open RAN. However, the use of SW makes Open RAN more vulnerable than RAN

owner to bypass the security system and obtain access to the system. This attack is possible after an already comprised hypervisor rollback to a previous snapshot. In the scheduler attack, the vulnerabilities in the hypervisor's scheduler are exploited to acquire system resources for the malicious VM at the expense of a victim VM (Yang and Fung, 2016; Khan et al., 2020).

Furthermore, due to virtualization and cloud computing, different applications might use the same hardware resources. Isolation between these applications is only at the software level and not at the level of hardware. As a consequence, hardware-related vulnerabilities like the recently discovered Meltdown and Spectre attacks (https://meltdownattack.com/) can have a larger attack range (Ericsson, 2020).

Finally, besides the main functionality of the VNF/CNF itself, the administrators may also decide to deploy additional network services on their VMs/CNs in order to do extra monitoring, remote configuration, remote access to other services such as SSH, etc. If these additional network services are directly accessible over the Internet or from another administrator, new entry points for attackers are created, and if access is obtained to the VM/CN, more extra attacks become possible (O-Ran Policy Coalition, 2021).

3.4. Global

Offering the highest level of security on the network is important for a nation. We here distinguish five major types of attacks or risks that need to be taken into account (Rasser and Riikonen, 2020). The related threats can be found in Table 7.

- **Attack on digital economy:** Since 5G is fully integrated into the digital economy, it can result in potential life-or-death consequences. For instance, currently, a lot of data is sent from our mobile devices, smart homes, and electrical cars via a network consisting of devices, which are remotely controlled and updated and thus present a potential attack vector. The possibility of a smart city shutting down, autonomous vehicles crashing, or factories going dark due to a cyber attack are frightening situations; that would eventually result in a major economic collapse. At this pivotal point in modern civilization where the global economic platforms are shifting to a holistic digital platform, a successful threat might endanger the entire growth of 5G and its predecessors through loss of trust from the subscribers. Thus, it is imperative to investigate the scope of such threat vectors that target economic platforms. It is evident the prescribed scope is reaching beyond the means of typical phishing, or identity thefts (Spremić and Šimunic, 2018). Moreover, the impending launching of Metaverse and its significance for O-RAN existence is further confirming the required focus on the robustness of digital economic platforms, as Metaverse is introducing a virtual serviceable platform built on top of monetary transactions (Chang et al., 2022).
- **Espionage:** There are currently no regulations for avoiding the collaboration between an Open RAN equipment manufacturer and an external party, like for instance a security agency of a certain country. Therefore, without a guarantee of good intentions of the equipment and software providers, possibilities for spying should be considered viable. Such acts of espionage can be perpetrated by targeting corporate to government institutions. The flexibility offered through O-RAN standardization might be

exploited, and privacy violations become the least of concerns for network operators. The AI-based decision making the backbone of the O-RAN architecture is inviting instilling of botnet-type autonomous constructs that entail a sophisticated cyber intrusion; where prevention is quite arduous (Bederna and Szadeczky, 2020). Therefore, proper ethical restraints should be drawn on a global scale to prevent such acts of espionage, while monitoring to detect such acts are equally pertinent.

- **Attacks on critical infrastructure:** Critical infrastructure typically consists of the management of power grids, water supplies, manufacturing, and transportation infrastructure. More and more, 5G is used as the backbone of communication in these infrastructures. Therefore, a dedicated cyber attack disrupting this critical infrastructure would have a devastating impact on the people dependent on this. Conversely, the control of the critical infrastructure is handed over to the 5G network operators. Therefore, their responsibility is ever so critical and honorable. Since the government level acts for blocking critical infrastructure to deliver threats in the geopolitical arena are not rare occurrences, O-RANs' dependence on the same network operators is raising concerns in the global shared resource market. Thus, the responsibilities of the network operators become extremely important within the O-RAN domain.
- **Violence against democracy:** If an actor receives the power to perform the role of big brother in all communication, there is a real threat to democracy and freedom of speech. As all the means of global economic infrastructure are envisaged to be shifted to a digital environment backed by the 5G-enabled networks, democracy becomes merely a concept without any context or standing in case of a total takeover. The ideals that made O-RAN more efficient and flexible might lead to the downfall of modern democracy and its stance on the global scale.
- **Majority attacks and supply chain concerns:** As mentioned in Braeke (2020) and Balding (2021), the Open RAN Alliance currently includes a wide range of high-security risk companies. If the efforts in the development and standardization process for Open RAN are dominated by partners belonging to one country or even one region, it can cause an imbalance resulting in a new alliance that will still enable espionage possibilities and disrupts the intended openness. As supply chains formed through globalization are relying on online trading and financial platforms for international transactions, the responsibility of the O-RAN stakeholders is ever so vital in facilitating the required digital infrastructure. It is obvious that Blockchain serves as an appropriate solution to secure such a financial infrastructure. The majority of attacks or 51% attacks are, however, proving to be realistic, where an attacker is capable of withdrawing the payment after the merchant has sent the product (Dey, 2018). This threat is intimidating the credibility of the Blockchain networks by enabling plausible deniability — which is one of its foremost purposes for the emergence of Blockchain.

4. Open RAN best security practices

We discuss the best security practices for Open RAN in this section. As Open RAN is a derivative of the conventional C-RAN, it will inherit many threats and vulnerabilities of C-RAN. Therefore, a number of C-RAN security solutions can be adopted by Open RAN without any significant modifications. For example, the existing security solutions to prevent primary user emulation attacks (PUEA) can be adopted for Open RAN (Tian et al., 2017). In Liu et al. (2010), the authors discussed cryptographic and wireless link signatures to distinguish between a legitimate user from an attacker. A helper node is proposed that is placed around a primary user. The helper node acts as a bridge between the primary and secondary users by sending authentic link signatures to the secondary nodes. The authors also proposed a corresponding physical layer authentication algorithm in Liu et al. (2010). There are other security mechanisms against PUEA based on the received signal strength. In Chen et al. (2009), the authors proposed naive detection and variance detection methods against PUEA. The authors modeled advanced strategies of PUEA where both the legitimate user and the attacker can exploit estimation techniques and learning algorithms. The variance detection attack is effective against PUEA for a time-invariant channel.

The most widely researched security threat in the medium access control layer is the spectrum sensing data falsification (SSDF) attack where an active attacker transmits error observation to disrupt collaborative spectrum sensing and resource allocation (Tian et al., 2017). A joint spectrum sensing and resource allocation scheme is proposed in Chen et al. (2016) to combat the SSDF attack. The problem is formulated as a weighted-proportional-fairness-based optimization problem with an additional constraint of the primary user being sufficiently protected. The authors decomposed the problem into two subproblems which are a resource allocation problem and a cooperative secondary user decision problem. The key idea of the scheme lies in improving the secondary users' sensing reliability and preventing the secondary user from acting maliciously. The computer simulations showed that the proposed scheme deals with the SSDF attack in the cooperative sensing process to improve system robustness.

As the Open RAN systems adopt cloud computing unlike conventional RAN systems, the security solutions for cloud computing are also relevant for Open RAN. In Xiao and Xiao (2012), the authors identified security and privacy vulnerabilities of cloud computing that can be exploited by an adversary for various attacks. The authors presented basic requirements to build a secure cloud system by addressing three main challenges, namely, outsourcing, multi-tenancy, massive data, and intense computation. To address the outsourcing challenge, the cloud provider needs to provide secure and trustworthy data storage. The outsourced data also needs to be verifiable by the customer. For multi-tenancy, the cloud platform needs to securely perform resource allocation in the virtualized environment. Finally, massive data sets need to be broken down into small sets to accelerate the processing. The solutions to PUEA, SSDF and cloud computing vulnerabilities are applicable to both C-RAN and Open RAN. We invite interested readers to go through Tian et al. (2017) for more discussion on the C-RAN security vulnerabilities and solutions.

We identify three key components to resolve security vulnerabilities that are exclusive to Open RAN. The first component to enhance Open RAN security is blockchain-based mutual authentication. As O-RAN promotes openness between a pool of untrustworthy O-RUs and O-DUs unlike C-RAN, the blockchain can be a very important and unique tool to establish trust between them and enable a safe communication mechanism. The second key component is the physical layer itself. The difference from other RAN systems is the operators have the option to select O-RUs from different competing vendors in Open RAN technology. Thus, the O-RUs can be installed at any moment with the desired number of antennas, front-end processing, and beamforming algorithms to enhance the security of the Open RAN. We also discuss RF fingerprinting techniques which can be crucial to identifying rogue RUs trying to connect to the system. The third key component is AI algorithms. As Open RAN provides more interfaces to enable an intelligent RAN system, we discuss a few examples of AI-enabled enhanced security in Open RAN. Table 8 summarizes the key solutions to threats and vulnerabilities related to Open RAN. Finally, we present a subsection regarding the common mistakes in Open RAN design, their consequences, and mitigation.

4.1. Blockchain-enabled Open RAN

Blockchain or distributed ledger technology (DLT) is a distributed database for exchanging identities of users and storing records of all user identities that are linked together using cryptography (Lipton

Table 8
Security solutions to Open RAN risks.

Threats and vulnerabilities	Solutions	Specific to Open RAN
Primary user emulation attack	A helper node can be used proposed which acts as a bridge between the primary and secondary user (Liu et al., 2010) or a variance detection method is adopted based on received signal strength (Chen et al., 2009)	No, applies to both C-RAN and Open RAN
Spectrum sensing data falsification	A weighted-proportional-fairness-based optimization problem can be formulated with an additional constraint of primary user being sufficiently protected (Chen et al., 2016)	No, applies to both C-RAN and Open RAN
Cloud computing vulnerabilities	A secure cloud system need to address three main challenges, namely, outsourcing, multi-tenancy, massive data and intense computation (Xiao and Xiao, 2012)	No, applies to both C-RAN and Open RAN
Untrustworthy O-DUs and O-RUs	A blockchain-enabled RAN framework can establish trust between untrustworthy O-DUs and O-RUs through a smart contract which is verified by third party miners (Ling et al., 2019)	Yes, only relevant to Open RAN due to its inherent openness
Privacy concerns in P2P communication	A distributed identity authentication through blockchain can enable privacy-preserving P2P communication without the involvement of certificate authority or public key infrastructure (Xu et al., 2021)	Yes, because Open RAN architecture enables different P2P communications such as D2D, M2M, etc.
Rogue O-RU	With prior knowledge of the transient and steady-state response of power amplifiers and other RF circuitry, RF fingerprinting techniques can determine whether an O-RU is rogue or benign (Soltanieh et al., 2020)	Yes, this threat is only relevant to Open RAN as it allows to integrate O-RUs from different vendors
Eavesdropping	Increasing the number of antennas and corresponding digital front-end processing with beamforming capabilities can diminish the threat of passive eavesdropping (Kapetanovic et al., 2015) and increase the probability of active attack detection (Schaefer et al., 2017)	Yes, the solution is O-RAN specific because the operator has the freedom to choose suitable O-RUs and O-DUs from different vendors in O-RAN
Conventional security framework	Open RAN enables intelligent zero-trust security framework upon which advanced AI algorithms can be developed to provide security in untrusted networks (Ramezanpour and Jagannath, 2021)	Yes, the proposed framework in Ramezanpour and Jagannath (2021) adopts service based design by leveraging Open RAN architecture to ensure ease of integration
DDoS attacks	Open RAN systems can employ machine learning algorithms that are trained to protect the network from DDoS attacks with very high accuracy (Doshi et al., 2018; Sharafaldin et al., 2019)	No, the machine learning solutions to detect DDoS attacks can be used by any RAN system

and Treccani, 2021). In other words, it is a chain of interconnected information blocks that creates a public ledger for recording a list of transactions. Blockchain is famous for its crucial role in modern cryptocurrency systems to provide a secure and decentralized record of transactions (ur Rehman et al., 2019). Blockchain, or DLT has also emerged as a tool for designing a self-organized and secure radio access network (RAN). Blockchain-enabled identity management and authentication can lower the cost and aid the core network to provide more secure and user-oriented service in an era of open and distributed RAN deployments (Hewa et al., 2022, 2020). In Ling et al. (2019), a RAN framework has been presented by leveraging the principles of blockchain. This framework proposes that the UEs and APs in the network agree about payments or spectrum assets based on a contract. The terms of this agreement are recorded by a smart contract, authorized by client signatures. Afterward, the contract is verified by the miners to determine whether the UEs have a sufficient credit balance or the APs have sufficient spectrum assets. The verified contracts are aggregated to a block, which is added to the existing blockchain. In this process, a UE will be granted limited-time access to the spectrum assets, while an AP can receive the payment automatically. As a result of enforcing the rights of relevant parties by means of a smart contract, trust has been established between initially untrustworthy UEs and APs. The application of blockchains and smart contracts for RAN can be further extended to cooperative communication, mobile ad-hoc networks, and privacy-preserving communication systems.

As RAN technology is moving towards more open, intelligent, virtualized, and interoperable networks in the form of Open RAN, it will be crucial to develop trust between a pool of O-RU and O-DU vendors. A blockchain-enabled smart contract establishes trust between these vendors and provides a mechanism to constantly monitor the development of the system by independent third parties. One such example is blockchain-enabled privacy-preserving point-to-point (P2P) communication in Open RAN. Due to the advent of distributed and decentralized functionality of Open RAN, different P2P communication in mobile networks, such as device-to-device (D2D) or machine-to-machine (M2M), will be beneficial. However, the fundamental security flaws for P2P communication in a mobile network will remain in an Open RAN. The P2P has limitations in global peer discovery and routing without third-party assistance, and thus, the coverage is a bottleneck. In the centralized architecture, the UE is restricted from communicating directly with other users. Two users under the same BS cannot be directly connected to each other without the involvement of the core network. The reason is several key functionalities, such as identity authentication, routing, etc., are only done at the core network in the state-of-the-art mobile networks. The distributed identity authentication issues in the current architecture can be addressed by blockchain due to its decentralized nature. The identity authentication can be performed locally at the RAN with a global identities record. In this way, two users under the same RAN unit can communicate with each other directly without accessing the core network.

In Xu et al. (2021), a blockchain-enabled mutual authentication architecture is presented for identity management in Open RAN that does not require a third-party Certificate Authority (CA) or Public Key Infrastructure (PKI). The authors proposed a blockchain address (BC ADD) as a global identity for all UEs within a RAN, where all users generate their own addresses by hashing their public keys. These newly generated addresses are recorded by the ledger records and used as anonymous identities locally or globally. The relationship

between the public key and BC ADD is strictly one-directional. As a result, it is difficult to fake a BC ADD when the public key is known or vice versa. The authors compared the performance of their proposed mutual authentication method based on blockchain with Internet Key Exchange version 2 (IKEv2) and Transport Layer Security (TLS) from signaling, communication and computation perspectives. The authors noted blockchain-based scheme only requires two signals, while IKEv2 and TLS 1.3 require 4 and 9 signals, respectively. The authors also demonstrated that the blockchain method requires significantly less number of bytes for finite-field and elliptic curve cryptography (ECC) for communication and computations. For communication, the blockchain method requires 1060 and 356 bytes for finite-field and ECC, respectively. The IKEv2 requires 3820 and 3110 bytes for finite-field and ECC, respectively, for the same functionality. Similarly, the number of bytes required for both finite-field and ECC is significantly higher for computation in IKEv2.

In Velliangiri et al. (2021), the authors presented a privacy-preserving framework of blockchain-enabled RAN for increased efficiency and enhanced security. The authors simulated their system model in Hyperledger Fabric 1.2-based simulator. The simulation shows that the blockchain-enabled RAN achieves higher throughput and lower resource consumption compared to conventional RANs. As Open RAN promotes open source software development for the base stations, it is imperative to develop a distributed security mechanism with *many eyes* to observe the changes in the Open RAN operation. Blockchain can provide an ideal framework to support RAN elements from different suppliers in a secured and organized manner. We believe blockchain can be a key element in future ORAN systems for authentication and identity management. However, several challenges remain to integrating blockchain technology into wireless networks. For power-limited node devices and cost-sensitive transmission networks, implementing blockchain-based mutual authentication can be challenging. In addition, latency can be a critical issue of blockchains for delay-sensitive scenarios in a wireless network. Despite these challenges, blockchain can be an important component of Open RAN systems as they suffer from more security challenges than traditional RANs due to their openness by design.

4.2. Leveraging physical layer to enhance Open RAN security

From an O-DU's perspective, it is crucial to differentiate a legitimate O-RU from a masquerading O-RU in the Open RAN systems. The transmitter of the O-RU consists of radio frequency (RF) modules such as digital-to-analog (DAC) converters, power amplifiers (PA), analog band-pass filters, frequency mixers, etc. Despite decades of research and development efforts by the microwave circuits community, long-standing imperfections still exist in the RF transmitter chain. These imperfections cannot be altered or corrected without significant effort and, thus, can be exploited as radiometric signatures of different O-RUs. In addition to conscious design decisions, these imperfections can stem from uncontrollable factors in the manufacturing process, such as differences in the semiconductor doping industry. As a result, different O-RUs can have very different flatness and ripples in the RF spectrum, differences in rejection and transition bands, mismatch in the I/Q phase, DC offset or gain imbalance, etc. The idea of using RF fingerprints to identify devices through such intrinsic features of the RF stages has been widely explored by the microwave circuit community. We believe such RF fingerprinting can also be used as the first line of defense to detect a masquerading O-RU.

A review of RF fingerprinting techniques has been presented in Soltanieh et al. (2020). The authors described state-of-the-art techniques for RF fingerprinting based on transient response. These methods utilize the transition from the turn-off to the turn-on of a power amplifier that occurs before the start-up of a radio unit. The transient response of every power amplifier is unique and, thus, can be used for wireless device identification. However, this method is effective when the transient is accurately known, i.e., the exact beginning and the exact end. The authors discussed several methods for detecting the start point of the transient, such as Bayesian step-change detection, Bayesian ramp-up change detection, phase detection, mean change point detection, etc. In Brik et al. (2008), the authors proposed an identification system based on the steady-state response of the hardware. The system is called a passive radiometric device identification system (PARADIS) and uses five features: frequency error, correlation, I/Q offset, magnitude errors, and phase errors to identify a device. As detecting the transient response requires a very high sample rate, which is infeasible in many applications, the steady-state response is frequently used for RF fingerprinting.

In Dolatshahi et al. (2010), a model-based approach is presented for the identification of wireless users via power amplifier imperfections. The authors exploited the differences in non-linearities of I/O characteristics of a power amplifier modeled with the Volterra series. The authors proposed a generalized likelihood ratio test (GLRT) and a classical likelihood ratio test to identify the legitimate user. A symbol-based statistical RF fingerprinting technique for fake base station identification is presented in Ali and Fischer (2019). The authors present a scheme to detect unique non-linearities based on the hardware impairments of the transmitter. The proposed scheme is based on the assumption that a fake base station tends to violate the spectral mark and introduces large amplitude and phase errors compared to a legitimate base station. RF fingerprinting can be an ideal mechanism to verify that an O-RU is secure enough to be connected to the O-DU of the O-RAN.

A massive multiple-input multiple-output (MIMO) O-RU can also improve the security of an Open RAN system. A massive MIMO system equips the base station with a large number of antenna elements that can serve a large number of user terminals in the same frequency band (Larsson et al., 2014). It should be noted that the antennas reside in the O-RU of Open RAN while the baseband layer processing is performed in the O-DU. The number of layers in the baseband is typically 16 or less in a 5G base station. For an N-layer O-DU, the O-RU must support at least a number of N antennas and RF-front-end circuitry. If the number of antennas in O-RU is significantly higher (e.g. 8–10 times) than N, the Open RAN system can be considered a massive MIMO system. Every layer of baseband data in the O-DU can exploit the higher number of antennas in O-RU with beamforming techniques. The base station can direct its baseband data in a specific direction by constructively adding multiple antenna streams and improving the signal quality. Due to their beamforming capability, massive MIMO systems are more secure than small-scale MIMO systems. It is possible to direct a narrow beam towards a legitimate user in a massive MIMO beamforming system. If an eavesdropper is not in the vicinity of the legitimate user, the received signal power of the eavesdropper is significantly diminished while the received power of the legitimate user increases manifold.

In Kapetanovic et al. (2015), the authors presented analytical results that showed a passive eavesdropper has a negligible effect on the secrecy capacity in a massive MIMO system. Their simulation shows that a passive eavesdropper's capacity remains the same with an increasing number of antennas. However, the legitimate user's capacity increases greatly for a large number of antennas. For a small-scale MIMO system with 2–8 antennas, the legitimate user's secrecy capacity is about half of the channel capacity. When the number of antennas is 100, the secrecy capacity reaches about 85 percent of the channel capacity. The primary reason for the resilience of a massive MIMO system against a passive eavesdropper is based on the assumption that the uplink channel estimation is independent of the eavesdropper's channel. However, an active eavesdropper can transmit pilot signals to the base station to influence them for transmitting beamforming design. In such a scenario, the physical layer security of a massive MIMO system is compromised, and the achievable secrecy rate vanishes with the increasing power of the eavesdropper's pilot signal. However,

the probability of detecting an attack increases with increasing eavesdropper's signal power (Schaefer et al., 2017). Two active eavesdropper detection methods have been proposed in Kapetanovic et al. (2015). The first scheme is based on random quadrature phase-shift keying (QPSK) pilot transmission by the legitimate user. The idea is that the phase of two legitimate pilot signals converges to valid PSK symbols as the number of antennas is large. In the second scheme, the beamformer is constructed in such a way that the received signal at the legitimate user is equal to an agreed value. These two detection schemes are only effective due to the large number of antennas in a massive MIMO system. Due to their centralized structure, the current base stations typically employ a fixed number of antennas and baseband layers. In the Open RAN design paradigm, the operators can select an O-RU with a higher number of antenna chains and, thus, with a capability to beamform and enhance security. We believe the ability to select O-RUs with the desired configuration will be crucial to improving the overall security of an Open RAN system. The most popular physical layer candidates for future wireless standards, such as cell-free MIMO or reflective intelligent surface (RIS) can utilize a high number of antennas. Thus, applying specific physical layer configurations is a viable solution to combat security threats such as eavesdropping in an Open RAN system. Identifying rogue O-RU will be crucial for Open RANs to succeed and replace conventional RANs. We believe RF fingerprinting could be the first line of defense against a rogue O-RU that is trying to connect to the network.

4.3. AI enabled Open RAN security

Since the introduction of deep learning by Hinton et al. there has been a reinvigorating interest in AI applications in the wireless communication research community. ML-based solutions have also been popular in the network security research community. Despite some security concerns associated with AI-based solutions, as mentioned before, the AI automated security solutions will represent an essential key element of future wireless networks. The application of AI is so crucial that entire security frameworks have been proposed to utilize AI algorithms. In Ramezanpour and Jagannath (2021), an architectural concept design of an intelligent zero trust architecture upon which advanced AI algorithms can be developed is proposed in order to provide security in untrusted networks. This framework adopts a service-based design by leveraging Open RAN architecture to ensure ease of integration. The three main components of zero-trust architecture in Open RAN are intelligent agent or portal (IGP), intelligent network security state analysis (INSSA), and intelligent policy engine (IPE).

The IGP employs a reinforcement learning approach to analyze the incoming traffic and provides an initial risk assessment and a model for their security posture. The reinforcement learning model used by multiple IGPs can be a common model that is trained in the federated learning approach. By utilizing federated learning, a more comprehensive model of the local environment is trained by different subjects. The second component INSSA provides a dynamic risk assessment for every access request. The authors proposed a graph neural network to model the state of Open RAN. The neural network models the communication patterns of the Open RAN with the goal of assigning risk scores in such a way that the overall security metric is maximized while granting access. The final component of the zero trust architecture in Open RAN is the IPE which makes the final decision to grant access. The IPE is based on a neural network called long short-term memory (LSTM) to evaluate the risk of granting access based on reports from IGPs and INSSA. After making a decision, the IPE monitors the security state of the session. The IGP, the INSSA, and the IPE work together to provide a cohesive framework for zero trust in Open RAN.

Conventional hardware-dependent security, such as firewalls or deep hardware inspections, might not be the ideal solution for a dynamic and open environment of Open RAN. Therefore, it would be crucial to develop automated mechanisms for intrusion detection, attack response, and mitigation. An Open RAN system can employ an ML mechanism that is trained to protect the network from DDoS attacks. A plethora of ML-based mechanisms for DDoS detection can be found in the literature. Five classification methods, including K-nearest neighbors (KNN), Decision Tree (DT), Random Forest (RF), Support Vector Machines with the linear kernel (L-SVM) and Neural Networks (NN) have been studied for intrusion detection in Doshi et al. (2018). The authors used a limited set of features to enable real-time classification and middlebox deployment. The authors found that all five methods were able to detect DDoS attacks with a high level of accuracy. However, the authors considered only three types of DDoS attacks. A total of 13 different DDoS attacks were considered in Sharafaldin et al. (2019). The accuracy of the ML algorithms decreased significantly for this scenario. In addition, both works of Doshi et al. (2018) and Sharafaldin et al. (2019) used supervised learning which requires labeled data. Such labeled data can be challenging to obtain, and thus, the application of supervised learning is not always realistic.

In Choi et al. (2019), the authors discussed network intrusion detection systems using different autoencoder architectures. Autoencoders are a type of artificial neural network based on unsupervised learning that aims to reconstruct its original input vectors. The proposed intrusion detection autoencoder develops a threshold heuristic of the reconstruction error, which represents the proportion of abnormality in training data. The authors considered four types of autoencoders, namely basic autoencoder, stacked autoencoder, denoising autoencoder, and variational autoencoder. The results showed that stacked and variational autoencoders perform better than the rest. A time-based anomaly detection system named Chronos is presented in Salahuddin et al. (2021). Chronos is an autoencoder that utilizes time-based features to detect anomalous DDoS traffic. This method extracts statistical information from time-based features for each small set of packets collected during a time window. The efficacy of Chronos was evaluated by performing extensive evaluations on the CICDDoS2019 dataset. The authors also evaluated the impact of different window sizes on detecting DDoS attacks. Chronos achieves an accuracy of over 99% for most attacks and greater than 95.86% for all attacks.

The application of AI for Open RAN security is not limited to intrusion detection. AI is an effective tool for identifying devices based on RF fingerprinting. Contrary to the hand-engineered approaches, the ML approaches are able to rapidly identify a rogue O-RU before sharing any network information. In Reus-Muns et al. (2020), the authors presented a convolutional neural network with a triple loss for RF fingerprinting. The authors demonstrated the feasibility of the proposed scheme over the experimental POWDER platform in Salt Lake City, Utah, USA. The proposed method achieves a 99.86% detection accuracy for different training and testing days on real-world datasets.

In Youssef et al. (2018), the authors studied four ML techniques to identify RF devices in the time domain. These four schemes are deep neural networks, convolutional neural networks, support vector machines, and multi-stage training using accelerated Levenberg–Marquardt. The authors examined data originating from 12 different transmitters. The accelerated Levenberg–Marquardt-based training method achieved 100% accuracy and outperformed state-of-the-art ML methods. A massive experimental study of deep learning for RF fingerprinting has been presented in Jian et al. (2020). The authors analyzed 400 GB of I/Q data transmitted by 10,000 radios. The authors chose convolutional neural networks because of their ability to interpret features better than conventional ML techniques. This work demonstrated that the proposed solution can handle different channel conditions and signal-to-noise ratios and is scalable to very large populations. It is almost certain that AI will play an integral role in the security of Open RAN systems. However, ML techniques themselves are vulnerable to security threats. The effectiveness of ML algorithms greatly depends on the quality of training data sets. An adversary can also send false data during the training process of the system. Therefore, robust ML algorithms that can tolerate malicious inputs need to be adopted. In addition, stability training can be adopted so that the ML schemes do not deteriorate for different and independent data sets.

Table 9
Overview of most common errors, consequences, and mitigation measurements.

General error	Consequences	Risk mitigation
Insecure design of Open RAN interfaces	Novel design strategies can be left with critical flaws due to the open and flexible approach of O-RAN (Mimran et al., 2022). Malware injection resulting in DoS attacks to retrieval of sensitive information via unauthenticated/unauthorized access (Burakovsky and Kriz, 2022).	Define security standards and protocols, as in Media Access Control Security (MACsec) for Open RAN devices and interfaces (Dik and Berger, 2021). Issue security certificates via standardized bodies. Train people to apply the defined standards and processes. Monitor network traffic for suspicious activity on all levels. Add firewalls and rate limiters to act appropriately. Proper Access control mechanism should be deployed as SbD (Klement et al., 2022).
Software flaws	Software for firewall protection can result in failures. The exploitation of buffer overflows results in the execution of arbitrary commands with devastating consequences.	Be careful with open-source software and keep software always up-to-date. Invest in security training for employees. Purchase software from trusted suppliers and use third-party certificate authorities. Follow the SDS approach for automating flaw detection (Harer et al., 2018; Chernis and Verma, 2018).
Insufficient protection of security event log files.	Security restoration delays, wrong audits, and threats persistence.	Automate the log monitoring process and add rate limits. Define log management clearly in the standard. SbD approach for automating log maintenance while introducing anomalous log detection using ML (Yadav et al., 2020; Klement et al., 2022).
Insufficient protection of data storage	Attacks against privacy, including data tampering, information disclosure, the elevation of privilege, etc.	MACsec protocol suite can be followed for the fronthaul, while an SDS-based approach can be deployed for the network and application layer network automation (Blanc et al., 2018; Klement et al., 2022). Follow data poisoning prevention methods (Desai et al., 2020).
Compromise of integrity and availability	DoS attacks. See also the consequences of the first error in case of improper authorization and authentication	A proper autonomous authentication and authorization mechanism is required to protect the integrity and ensure availability (Ramezanpour and Jagannath, 2021).
Physical access	Retrieval of stored private keys, certificates, user plane data, control plane data, and management data in cleartext. Modification of Open RAN components settings and configurations in order to disable security features and allow eavesdropping or wiretapping on various planes, creates performance issues (Ericsson, 2020).	Define security standards for physical security. Ensure that all stakeholders in the Open RAN system are identified, authenticated, and trusted (Amy Zwarico et al., 2020).

4.4. General mistakes, consequences, and mitigation

Almost all of the technology-related attacks mentioned in Section 3.3 are caused because of some general design errors. Table 9 summarizes these major errors, together with their consequences and potential mitigation measures.[1]

The following six general mistakes are identified.

- ***The hardware-software Open RAN system suffers from insecure design:***
  The open fronthaul and its interfaces, xApps-based radio resource management, Decoupled hardware, open management interfaces, and open source deployments are some insecure design strategies that require more investigation to determine remedial possibilities (Mimran et al., 2022). This includes misconfigured or poorly configured Open RAN interfaces due to outdated components or improperly configured permissions, insufficient/improper mechanisms for authentication, encryption, and authorization in different hardware-software components of the Open RAN system.
  This type of weakness would allow attackers to inject malware in order to manipulate and harm the Open RAN components, which may result in a variety of consequences going from launching DoS attacks to retrieval of sensitive information including unprotected private keys. As a consequence, the attacker gets unauthenticated/unauthorized access to Open RAN components via the different Open RAN interfaces.
  In order to offer protection against this, security standards (e.g. Media Access Control Security — MACsec) for Open RAN devices and interfaces should be clearly defined and people should be trained in order to apply these standards and processes (Dik and Berger, 2021). In particular, special attention should be given to all access control mechanisms at every access point. A Security by Design (SbD) approach might be suitable for automating the authorization framework (Klement et al., 2022). Security certifications should be issued via trusted security standardization bodies. It is also essential to monitor network traffic for suspicious activity on all levels and to add firewalls and rate limiters to act appropriately.
- ***Software flaws:*** The tendency to utilize open source solutions for virtualization deployments as well as for the RU, DU, and CU-based deployments is a way to assert the required interoperability within a multi-vendor O-RAN; At the same time exposes the software specifications and configurations to the general public (Mimran et al., 2022). This opportunity allowing the assimilation of the software standards would benefit either negatively or positively depending on the capability of the attacker or the defender. Software flaws are present in the different components of the Open RAN system, which are not notified and mitigated in time.
  In particular, software-providing network functionalities play an important role in firewall protection. If vulnerabilities like buffer overflows are exploited, arbitrary commands can be executed with devastating consequences.
  As Open RAN is built with open-source software, it is important to keep the software always up-to-date and to make sure that they are developed by trusted suppliers, which use third-party certificate authorities. Security training for employees is required such that software is developed with the highest standards. Further, the Software Defined Security (SDS) concept can be extended to the application layer from the network layer for automating the security functions and detecting software-based flaws through machine learning means (Chernis and Verma, 2018; Harer et al., 2018).
- ***Security event log files, generated by the different Open RAN components, are not sufficiently or improperly protected:*** Security has not been recognized as a function by the O-RAN setup

[1] Note that these mitigation measures are closely related to the process-related risks, which can in fact also be considered as guidelines (see Table 2).

to maintain proper and organized logs for event recording. For instance, they lack information on hostname, IP or MAC address, correct timing of incidents, etc.
Compromise or incomplete logs can result in security restoration delays, wrong audits, and threats persistence.
The standard should clearly define how to manage the log monitoring process and rate limits should be added. SbD approaches can be employed for centralized log auditing, while an automated anomalous detection method for security logs can be an efficient directive to overcome this pitfall (Yadav et al., 2020; Klement et al., 2022).

- ***Sensitive data, stored, processed and transferred among the different Open RAN components, are not secured according to industry best practices:*** For instance, appropriate encryption and integrity protection mechanisms are missing, inappropriate access control, lack of traceability of the access in the audits, etc.
  This weakness will mostly result in attacks against privacy, including data tampering, information disclosure, the elevation of privilege, etc.
  Security standards for authentication and end-to-end encryption (MACsec) following the latest developments should be defined (Dik and Berger, 2021). Security certifications should be issued via security standardization bodies. People should also be trained to apply the defined standards and processes. Finally, data poisoning prevention algorithms should be deployed (Desai et al., 2020).
- ***Integrity and availability of Open RAN components can be compromised:*** Integrity and availability of Open RAN components can be compromised due to overload situations caused by DoS attacks or increased traffic and where the Open RAN components do not possess the required functionalities to deal with it.
  A direct consequence is of course a DoS attack. However, other possibilities may appear in case of insufficient or improper configuration (see the first error). For instance, an attacker might be able to boot Open RAN components from unauthorized memory devices and thus instill a selected malware to a xApp or any other operational entity (O-Ran Policy Coalition, 2021).
  Similar countermeasures as in the previous mistake should be taken.
- ***Several possibilities allow physical access to different components in the Open RAN system:*** First, it can appear via ports and consoles (such as JTAG, serial consoles, or dedicated management ports) which are insufficiently secured. Second, the credentials of the administrator may be insufficiently protected. Another possibility is that the configuration module of the hardware and software might be insufficiently protected against malware injection and manipulation.
  Physical attacks on the Open RAN deployment enable the retrieval of stored private keys, certificates, user plane data, control plane data, and management data in cleartext. Moreover, attackers can try to modify the Open RAN components settings and configurations via local access in order to disable security features and allow eavesdropping or wiretapping on various planes, creating performance issues (Ericsson, 2020).
  Also for physical access, the required security standards should be developed. In addition, all stakeholders in the Open RAN system need to be identified, authenticated, and trusted (Amy Zwarico et al., 2020).

5. Security benefits of Open RAN

Besides all these risks, Open RAN brings of course a whole series of benefits. Several benefits are typical for Open RAN, others are also available in V-RAN and some of them are common for all 5G networks. Table 10 provides an overview of the main benefits.

5.1. Open RAN specific

5.1.1. Full visibility

Due to virtualization and the disaggregated components connected through open interfaces, operators have direct access to all network performance data and operational telemetry data representing activities between/within the different network functions. The integrity of this data is ensured as this data is created isolated from the functions' executing environment. Combining this data with security log data results in earlier detection of security problems and easier detection of the root cause (O-Ran Alliance Security Focus Group, 2021a; Hanselman, 2020; Redhat, 2020).

Note that full visibility can also be a risk. Due to the complexity, the root cause cannot always be easily detected and there is a danger that different vendors will not take accountability for potential issues. Following Weissberger (2021), it is claimed that the time and cost to perform a complete security review would seem to be multiplied by the number of vendors the operators take on board.

5.1.2. Selection of best modules

Operators can more easily select the vendors offering the best products, meeting the required industry security standards and certifications (O-Ran Alliance Security Focus Group, 2021a; Hanselman, 2020; Redhat, 2020). Examples of industry best practices are for instance "secure by design" DevSecOps in which information security operations are integrated into DevOps workflows and automated testing in the development of containerized applications (Hsu, 2018). The operator can also collaborate with the vendor to determine and influence Continuous Integration/Continuous Deployment (CI/CD) processes with continuous regression testing and software security auditing used by the supplier. Other good practices are the adoption of Supplier Relationship Management (SRM) with an inbound development process and strict security controls for Free and Open Source Software (FOSS), trust stack management with software coming from reliable supply chains and trusted, well-defined operations, intelligent vulnerability management, and multi-vendor System Integration (SI) with continuous verification on vendors sharing the same interpretation and implementation of functions (O-Ran Alliance Security Focus Group, 2021a; Altiostar, 2021).

There are a range of industry best practices that can be adopted including Groupe Speciale Mobile Association (GSMA), National Institute of Standards and Technology (NIST), European Union Agency for Cybersecurity (ENISA), National Telecommunications and Information Administration (NTIA), Center for Internet Security (CIS), Open Web Application Security Project (OWASP), Open Standards, Open Source (OASIS), national cyber security organizations, Building Security In Maturity Model (BSIMM), Cloud Native Computing Foundation (CNCF), the Linux Foundation, SAFECode and CNTT (Hanselman, 2020; Redhat, 2020).

5.1.3. Diversity

Integrating independent and individual modules decreases the risk that common coding errors or practices of one single entity impact large parts of the network and thus decrease the attack range. Consequently, diversity helps to balance the security risks. Open RAN enables an expanded pool of vendors on the market, reducing a nation's dependence on any sole vendor for wireless services (Hanselman, 2020; Docomo, 2021; Software org, 2021). Despite the O-RAN entities being contrived following common and established standards, multiple vendors might embed diverse mechanisms, and technologies to meet the standards or guarantees. This will eventually create competition among the vendors for better market returns. This competition can be considered healthy from the security perspective, as the standards might have to be improved from the security front to convince the consumers.

Table 10
Overview of Open RAN benefits.

RAN type	Benefit	Short description
Open RAN specific	Full visibility	The operator has increased visibility, allowing better security control and response to incidents (O-Ran Alliance Security Focus Group, 2021a; Hanselman, 2020; Redhat, 2020).
	Selection of best modules	Operators will be able to integrate best-in-class security platforms (O-Ran Alliance Security Focus Group, 2021a; Altiostar, 2021; Hanselman, 2020; Redhat, 2020; Docomo, 2021; Ericsson, 2020).
	Diversity	Diversity and independency among the diverse modules will decrease the attack range (Hanselman, 2020; Docomo, 2021; Software org, 2021).
	Modularity	Enabling more efficient, seamless patch management and SW updates to remove vulnerabilities [] (O-Ran Alliance Security Focus Group, 2021a; Redhat, 2020).
	Enforcement of security controls	Security controls can be better enforced (Altiostar, 2021).
	Open interfaces	Operators are independent of the supplier to react to security issues (Masur et al., 2022; Docomo, 2021; Hanselman, 2020).
	Open source software	Open source software has been verified by multiple parties (Masur et al., 2022).
	Automation	The complete automation of network management can be accelerated (O-Ran Alliance Security Focus Group, 2021a; Masur et al., 2022; Docomo, 2021).
	Open standards	Better coordination of security measures become possible (O-Ran Alliance Security Focus Group, 2021a; Hanselman, 2020).
V-RAN	Isolation	Isolation enables more control and fewer issues during updates for security management (Hanselman, 2020).
	Increased scalability	It enables better trade-offs between performance and security (Hanselman, 2020).
	Control trust	Operators are able to control full trust in their network (Hanselman, 2020).
	Less dependency between HW and network SW	There are fewer risks for SW upgrades (Redhat, 2020).
	Private networks	There is easier migration to private networks (Redhat, 2020; Johnson, 2020).
	More secure storage of key material	More secure storage of key material (Redhat, 2020).
5G	Edge oriented	Security is dealt with closer to the edge of the network in order to stop attacks closer to the source (O-Ran Alliance Security Focus Group, 2021a).
	Simpler security model	The zero trust security principle can be implemented (O-Ran Alliance Security Focus Group, 2021a).

5.1.4. Modularity

Due to the modularity of the network, operators can switch to a CI/CD operating model, enabling seamless and effective patch management for fixing any detected security vulnerability. As a consequence, the vulnerabilities in the network are faster removed. In addition, updates become more transparent and have less impact on the overall network. Moreover, also operational agility is obtained making it possible to replace functional elements with new versions or capabilities (O-Ran Alliance Security Focus Group, 2021a; Redhat, 2020). The CI/CD method combined with the DevSecOps principles can insure individual modules carry out the updates or patches separately, eliminating any opportunity for complete compromise of the system in case of a malicious agent was conveyed via the updating process (Lee et al., 2021b).

5.1.5. Enforcement of security controls

Due to the choice among different vendors, modularity, and open interfaces, the operator is in the position to demand strong security capabilities and control of its suppliers. For instance, in the case of cloud architecture, the operator and the cloud infrastructure supplier have a common agreement in which this last one is responsible for the deployment of the latest security tools for detection and prevention (Altiostar, 2021; Hanselman, 2020).

5.1.6. Open interfaces

Open interfaces at the different levels give a higher exposure, resulting in more scrutiny and thus higher overall security. Thanks to the open interfaces, operators are not dependent anymore on the supplier in case of (security) issues and can do upgrades themselves, being able to react faster. It also gives the possibility to experiment with new functions and new vendors, exploring new ways to secure the network and its operation (Masur et al., 2022; Docomo, 2021; Hanselman, 2020). This is at the same time a risk as in order to explore new possibilities by the operator, sufficient qualified people are required, which is not evident due to the complexity of the overall system.

5.1.7. Open source software

Open-source software presents security challenges regarding its open nature but has the advantage of being verified by multiple independent parties, being rigorously and varied tested, and customized against threats (Masur et al., 2022).

As mentioned before, the use of open source also includes many risks. It was concluded in the GitHub 2020 State of the Octoverse Report that vulnerabilities remain undetected in many cases for more than four years, before being disclosed (Bakhitova, 2020). Therefore, one cannot simply state that open-source software is faster patched than proprietary software.

5.1.8. Automation

The introduced intelligence in Open RAN can be used to automate management and control via big data analysis, AI, and ML. As a consequence, closed-loop responses to changes in the network can be automatically performed. This has the advantage that no human interactions are required anymore, which inherently includes threats like humans accidentally altering the security posture of a network function or maliciously harvesting credentials, changing configurations,

or implanting malware within the network (O-Ran Alliance Security Focus Group, 2021a; Masur et al., 2022; Docomo, 2021).

Again, automation can bring risks as previously identified in the ML algorithms.

5.1.9. Open standards

Open RAN will be developed based on open standards, defined by the Open RAN consortium. Such standards enable to align on a common approach approved by leading members in the field and coordinate all information regarding security threats, vulnerabilities, and exploits (O-Ran Alliance Security Focus Group, 2021a; Hanselman, 2020).

A prerequisite is of course the presence of these standards, which are not fully available at the moment. In addition, these standards should be correctly implemented.

5.2. V-RAN specific

5.2.1. Isolation

Isolation is obtained via the defined interfaces between functional elements in an Open RAN. It offers on the one hand the possibility to insert controls for monitoring and on the other hand, allows software updates and patches to be installed with less risk that version dependencies will create issues (Hanselman, 2020; Gavrilovska et al., 2020).

5.2.2. Increased scalability for security management

Often, there are trade-offs between application, performance, and security requirements. Due to the modularity, operators can tailor their deployments and shift more easily the resources for monitoring and control to meet better to these requirements and improve scalability (Moreira et al., 2021). Also, vRAN functional elements can be shifted to provide better isolation (Hanselman, 2020).

5.2.3. Control trust

Since operators control the platforms on which virtualized functions run in Open RAN, they have also complete control of the trust infrastructure (Benzaïd et al., 2021). The identity and provenance of each functional element are known and managed by using strong cryptographic mechanisms like signature operations. Each new version is validated by the operators and therefore have control over what is, and where it is running on their networks (Hanselman, 2020).

However, it must be taken into account that the situation becomes more complex as there are more assets and stakeholders involved.

5.2.4. Less dependency between HW and SW

In an Open RAN, there is less dependency between the network software and hardware. This makes it in the first place easier to perform the required upgrades in a faster way. Second, it also avoids risks associated with isolated security breaches (Redhat, 2020; Gabilondo et al., 2022).

5.2.5. Private network

Private 5G networks will soon become the general trend as they enable companies the possibility to fully customize the network according to their specific needs with respect to speed, bandwidth, security requirements, on their locations, and own timetable. It will enable companies to offer their customers a dedicated 5G experience, with applications in a large range of domains from healthcare, manufacturing, transportation, education, etc. Companies will have the option to build out and run their own private 5G network, or they can also outsource it to a mobile network operator or systems integrator (Verizon, 2021). One such option is via network slicing, where each slice can be seen as a complete end-to-end network and includes the security capabilities according to the needs (Redhat, 2020).

There will be soon many players on the market to launch this innovative network as a service concept, replacing in many cases their existing Wi-Fi and fixed wireless/wired infrastructure.

5.2.6. More secure storage of key material

In traditional network architectures, sensitive cryptographic key material such as for instance Access Stratum keys are more vulnerable to various threats as they are stored at the cell site (Cichonski, 2020). In Open vRAN, this key material can be stored deep inside the network in a secure vCU, hosted in a data center (Redhat, 2020).

5.3. 5G networks related

5.3.1. Edge oriented

Due to the open interfaces, the operator is able to spread the security analysis throughout the network and include monitoring at the edge. These edge-focused analytics will facilitate the detection and prevention of attacks at the lower part of the network in order to avoid DDoS and block malicious data from reaching the core network. This is, in particular, important to support mobility services like services offered by IoT (O-Ran Alliance Security Focus Group, 2021a; Ge et al., 2017).

5.3.2. Simpler security model

In zero trust (Rose et al., 2020), nothing is trusted unless it is verified, regardless of the location. The O-RAN Alliance completely embraces this principle. Therefore, everything needs to be verified and results need to be communicated (O-Ran Alliance Security Focus Group, 2021a). Zero-trust networking can enhance security in different domains by relying on robust standards. First, it secures the technology and application stack including all interfaces and APIs. Second, it allows the leverage of the cloud-based nature of 5G and the deployment of cloud security functionality and telemetry. Third, it ensures the tailoring and customization of the security control via network slicing. Finally, it makes it possible to deploy multiple layers of authentication (Liyanage et al., 2022).

6. Lessons learned and discussion

6.1. Lessons learned

In this section, we summarize the key lessons learned from previous sections of this survey.

6.1.1. Threat vectors and security risks associated with Open RAN

We have provided a clear taxonomy and an extensive overview of the different types of risks in Open RAN. There are basically three main domains of risks: process, technology, and global. The global risks are general and apply to any type of RAN. In particular, we have shown that most of the technical risks follow from basic errors like insufficient mechanisms for encryption, authentication, and authorization, improper configuration, software flaws, inappropriate event log management, lack of integrity and availability protection, and unprotected physical access. Corresponding risk mitigation measures are provided, which are also related to the identified process risks. Basically, it all falls or stands with well-defined standards and policies on all different processes covering the complete lifecycle, which can be clearly implemented, verified, and audited in an automatic way. This is currently ongoing work, but progress is on the way.

6.1.2. Open RAN best security practices

As a derivative of C-RAN, Open RAN can inherit many security solutions and practices straight from C-RAN (Morais et al., 2020; Gavrilovska et al., 2020). However, due to its open architecture, it also requires a significant number of unique security solutions. Most such solutions are required due to their lack of restrictions on O-RUs from different vendors. Open RAN enables blockchain-based mutual authentication and privacy-preserving P2P communication. Unlike conventional RAN technologies, Open RAN platforms can be upgraded with beamforming functionality and provide a countermeasure against

eavesdroppers. Open RAN provides a platform to utilize the full benefit of AI algorithms for security solutions. In addition, many technology-related attacks are caused by general design errors and can be mitigated by defining security standards and automation.

6.1.3. Security benefits of Open RAN

A significant amount of additional security benefits have been identified for Open RAN, compared to v-RAN and even 5G networks. However, most of them are closely related to security risks. For instance, full visibility, selection of best modules, diversity, modularity, and open interfaces also bring increased complexity and interdependency, requiring sufficiently trained people and trusted stakeholders. The same holds for open-source software, which clearly has several advantages, but also brings several risks, as identified here. Another example is the possibility of creating an advanced level of automation in the network, but at the same time can lead to vulnerabilities from potential AI/ML attacks. Finally, for the enforcement of security controls and the adoption of open standards, the required standards, processes, and policies still need to be fully defined.

6.2. Discussion

6.2.1. Cost of security in O-RAN deployments

The RAN section of the telecommunication domain typically costs around 70% to 80% of the entire cost of the network, and it represents the best opportunity to reduce the cost of the network. In comparison, O-RAN is more economically beneficial than PHY-RAN or vRAN. The openness of the O-RAN is inviting the vendors to be more competitive with their apparatus, where 30% less amount can be expected on Open Radios and O-RAN software. As proprietary BBUs are replaced by the typical servers, their cost becomes less in comparison. According to Fetterolf (2021), 32.5% Capital Expenditure (CapEx) savings and 21% Operational Expenditure (OpEx) savings can be expected regardless of whether the O-RAN is configured D or C setting. O-D-RAN, in contrast to O-C-RAN, has higher CapEx and OpEx values.

The major security repercussions of the O-RAN deployments are forecasted due to its openness of interfaces and modules. Ramifications for such flaws are typically automated security solutions or standards that define secure protocols for communication channels that cover confidentiality, integrity, and accountability; and an automated access control scheme. In addition, an AI or ML-driven firewall and IDS facilities are imperative for securing the subdomains. Even with the highest level of cryptographic primitives, the computation power required for secure communication protocols can be managed within the available O-RAN resources. The security overhead applicable to the channels is aggregated to the OpEx. The service-oriented 5G networks are offering most of their services as cloud-based services. Security can also be offered as a service where access control framework, firewall, and IDS facilities can be different flavors of the Security as a Service (SECaaS) use case (Ranaweera et al., 2020). These cloud-oriented edge-leveraged services eliminate the requirement for dedicated hardware and nullify the required CapEx for launching SECaaS. Such a service can be purchased as a subscription-based service that covers the entire O-RAN fronthaul domain, and it can be shared among the other O-RAN services. Hence, OpEx can be manageable. This service outsourcing will allow dynamic scaling ability. For security management and orchestration, however, an agent of the SECaaS service should be deployed within the O-RAN for monitoring the security-related actions and responses. A substantial amount of CapEx should be allocated for this agent as it requires to be high performing. Considering all these aspects where CapEx and OpEx are allocated, the cost does justify the benefits granted through the SECaaS-based services that would mitigate any disruptions to the O-RAN system.

6.2.2. Impact of quantum computing

Quantum Computing (QC) represents a superior computing power that exceeds almost 158 million times faster than a state-of-the-art supercomputer (Floridi, 2021). The QC manifests an amalgamation of quantum mechanics of superposition, interference, and entanglement. The models that form the QC computations are often based on quantum bits (qbits), where the qbit value scopes higher than a typical computing bit, with its states. With this enormous computing power, QC is an obvious candidate for O-RAN processing core components, specifically for RIC-based computations. A QC-enabled core RIC can deliver the real-time outcomes of the Near-RT services. In spite of its power, QC-based computing requires unique models for performing computing operations. Typical radio resource management and allocation computations might have to adhere to QC models or algorithms for solving the problems.

From the perspective of security, QC is a technology that challenges the complexity of modern applied cryptographic algorithms (Jurcut et al., 2020). The RSA algorithm, which is believed to be unbreakable in the current context, can be broken with a QC employing Shor's algorithm factoring discrete logarithms. Thus, QC poses a threat to the security of future networks and systems despite its rare existence. As a solution, Quantum Resistance (QR) cryptography was introduced and bares a significant interest among the research community. QR algorithms can be formulated from lattice-based, multivariate, hash-based, or elliptic curve-based methods (Ranaweera et al., 2021). Thus, O-RAN can leverage the capabilities offered through QC to achieve the guaranteed service level requirements. A Quantum Key Distribution (QKD) infrastructure can be adopted as the PKI for O-RAN internal entities, including the xApps and rApps. On the contrary, QR-based defense mechanisms should be adopted for signaling and critical channels for improving both the security and efficiency of the O-RAN.

6.2.3. Role of securing B5G/6G applications

Metaverse is a concept introduced to transcend physical space into a digital reality where all the possible actions in the real world are enabled within the digitized world. Though the technologies Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR), and Extended Reality (XR) are available, a holistic solution that incorporates all these digital visualization technologies is lacking (Lee et al., 2020). Metaverse satisfies that void and envisages possibilities beyond measure. The network bandwidth, latency, jitter, availability, and reliability aspects of the RAN should be at its highest capacity to deliver a successful Metaverse (Lee et al., 2021a). In addition, a significant level of interoperability and flexibility should be maintained within the network to guarantee performance with haptic sensory feedback. The O-RAN is capable of delivering the required flexibility and interoperability within its network. The security concerns of the Metaverse mostly exist in the virtual domain. Therefore, O-RAN cannot guarantee the internal security of the Metaverse; but can secure the network domain via typical security mechanisms.

Digital Twin (DT) technology contrives an exact replica of an object in the digital space. The replica or the twin, however, is formed in a simulated environment where all the actions committed by the actual object and its reactions can be mimicked on its digital counterpart (Jones et al., 2020). The main purpose of a DT application is to enable remote controlling and monitoring of apparatus or equipment situated in a factory environment aligned with Industrial IoT (IIoT) deployments (Ranaweera et al., 2022). The DT concept can be visualized as a miniature version of the Metaverse, where an interactive interface is formed through AR-based collaborative tools. The O-RAN dynamic and flexible launching of xApps, with their Near-RT standards, can facilitate the DT applications successfully. It requires lesser network-based requirements than Metaverse. Though, the service rendered by the DT can be most critical and require dedicated service channels with priority. Thus, fronthaul communication channels should embed better security credentials for DT deployments.

7. Conclusion

In order to cope with the continuous growth of mobile subscribers, mobile data, and mobile services, a drastically new approach is needed in order to ensure that the network resources are used in the most optimal way. In addition, this solution should particularly take into account thorough security protection as also the amount and impact of cybersecurity attacks are continuously increasing.

Open RAN offers all the possibilities to enable a great breakthrough in the network technology landscape and is able to address most of the current shortcomings in RANs thanks to the added openness and intelligence. However, due to this totally new approach, where multiple vendors can now simultaneously integrate their technology, a more complex ecosystem exists, resulting in a multitude of new risks and opportunities. We have provided a comprehensive overview of these different risks and benefits. We also discussed the best security practices to be applied. As an important conclusion, in order to fully benefit from the essential opportunities and to avoid the most important risks, the existence of an extended standard describing in detail the different processes in Open RAN is an essential step.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

This work is supported by 6Genesis Flagship (grant 318927) project. The research leading to these results partly received funding from European Union's Horizon 2020 research and innovation program under grant agreement no 101021808 (H2020 SPATIAL project). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains.

References

Abdalla, A.S., Upadhyaya, P.S., Shah, V.K., Marojevic, V., 2021. Toward next generation open radio access network–what O-RAN can and cannot do!. arXiv preprint arXiv:2111.13754.

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., Gurtov, A., 2018. Overview of 5G security challenges and solutions. IEEE Commun. Stand. Mag. 2 (1), 36–43.

Ali, A., Fischer, G., 2019. Symbol based statistical RF fingerprinting for fake base station identification. In: 2019 29th International Conference Radioelektronika (RADIOELEKTRONIKA). pp. 1–5.

Alina, A., Saraswat, S., 2021. Understanding implementing and combating sniffing and ARP spoofing. In: 2021 4th International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE). IEEE, pp. 235–239.

Alnaim, A.K., Alwakeel, A.M., Fernandez, E.B., 2019. A misuse pattern for NFV based on privilege escalation. In: Proceedings of the 8th Asian Conference on Pattern Languages of Programs.

Altiostar, 2021. Security in Open RAN. White Paper, doi:https://www.altiostar.com/white-paper-security-in-open-ran/.

Amy Zwarico, S.J., et al., 2020. The O-RAN ALLIANCE Security Task Group Tackles Security Challenges on All O-RAN Interfaces and Components. Blog.

Bakhitova, A., 2020. Analysis of newcomers activity in communicative posts on GitHub. In: Digital Transformation and Global Society: 4th International Conference, DTGS 2019, St. Petersburg, Russia, June 19–21, 2019, Revised Selected Papers, Vol. 1038. Springer Nature, p. 452.

Balasubramanian, B., Daniels, E.S., Hiltunen, M., Jana, R., Joshi, K., Sivaraj, R., Tran, T.X., Wang, C., 2021. RIC: A RAN intelligent controller platform for AI-enabled cellular networks. IEEE Internet Comput. 25 (2), 7–17.

Balding, C., 2021. Revisiting the United States telecommunications network policy in a post-huawei world: Improving economic competitiveness, addressing security weakness, and building alliances.

Batalla, J.M., Andrukiewicz, E., Gomez, G.P., Sapiecha, P., Mavromoustakis, C.X., Mastorakis, G., Zurek, J., Imran, M., 2020. Security risk assessment for 5G networks: National perspective. IEEE Wirel. Commun. 27 (4), 16–22.

Bederna, Z., Szadeczky, T., 2020. Cyber espionage through Botnets. Secur. J. 33 (1), 43–62.

Benzaïd, C., Taleb, T., 2020. AI for beyond 5G networks: a cyber-security defense or offense enabler? IEEE Netw. 34 (6), 140–147.

Benzaïd, C., Taleb, T., Farooqi, M.Z., 2021. Trust in 5G and beyond networks. IEEE Netw. 35 (3), 212–222.

Berkeley, A.R., Wallace, M., Coo, C., 2010. A Framework for Establishing Critical Infrastructure Resilience Goals. Final Report and Recommendations By the Council, National Infrastructure Advisory Council, pp. 18–21.

Bitsikas, E., Pöpper, C., 2021. Don't hand it over: Vulnerabilities in the handover procedure of cellular telecommunications. In: Annual Computer Security Applications Conference. pp. 900–915.

Blanc, G., Kheir, N., Ayed, D., Lefebvre, V., de Oca, E.M., Bisson, P., 2018. Towards a 5G security architecture: Articulating software-defined security and security as a service. In: Proceedings of the 13th International Conference on Availability, Reliability and Security. pp. 1–8.

Bobrovskis, S., Jurenoks, A., 2018. A survey of continuous integration, continuous delivery and continuos deployment. In: BIR Workshops. pp. 314–322.

Bonati, L., Polese, M., D'Oro, S., Basagni, S., Melodia, T., 2022. OpenRAN gym: An open toolbox for data collection and experimentation with AI in O-RAN. arXiv preprint arXiv:2202.10318.

Booth, H., Rike, D., Witte, G.A., et al., 2013. The national vulnerability database (nvd): Overview.

Braeke, D., 2020. A US National Strategy for 5G and Future Wireless Networks. Information Technology and Innovation Foundation (ITIF).

Brandão, A., Resende, J.S., Martins, R., 2021. Hardening cryptographic operations through the use of secure enclaves. Comput. Secur. 108, 102327.

Brik, V., Banerjee, S., Gruteser, M., Oh, S., 2008. Wireless device identification with radiometric signatures. In: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. pp. 116–127.

Bugár, G., Vološin, M., Maksymyuk, T., Zausinová, J., Gazda, V., Horváth, D., Gazda, J., 2020. Techno-economic framework for dynamic operator selection in a multi-tier heterogeneous network. Ad Hoc Netw. 97, 102007.

Burakovsky, L., Kriz, D., 2022. The imperative of enterprise-grade security for 5G. Cyber Secur.: Peer-Rev. J. 5 (4), 303–315.

Carlson, J.M., 2021. Ericsson Open RAN FCC reply. GN Docket No. 21-63.

Chang, L., Zhang, Z., Li, P., Xi, S., Guo, W., Shen, Y., Xiong, Z., Kang, J., Niyato, D., Qiao, X., et al., 2022. 6G-enabled edge AI for metaverse: Challenges, methods, and future research directions. arXiv preprint arXiv:2204.06192.

Chen, Z., Cooklev, T., Chen, C., Pomalaza-Ráez, C., 2009. Modeling primary user emulation attacks and defenses in cognitive radio networks. In: 2009 IEEE 28th International Performance Computing and Communications Conference. IEEE, pp. 208–215.

Chen, S., Jia, R., Qi, G., 2020. Improved techniques for model inversion attacks. abs/2010.04092.

Chen, H., Zhou, M., Xie, L., Wang, K., Li, J., 2016. Joint spectrum sensing and resource allocation scheme in cognitive radio networks with spectrum sensing data falsification attack. IEEE Trans. Veh. Technol. 65 (11), 9181–9191.

Chernis, B., Verma, R., 2018. Machine learning methods for software vulnerability detection. In: Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics. pp. 31–39.

Chi, Z., Li, Y., Liu, X., Wang, W., Yao, Y., Zhu, T., Zhang, Y., 2020. Countering cross-technology jamming attack. In: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks. pp. 99–110.

Choi, H., Kim, M., Lee, G., Kim, W., 2019. Unsupervised learning approach for network intrusion detection system using autoencoders. J. Supercomput. 75 (9), 5597–5621.

Cichonski, J., 2020. 5G Security-Evolution not Revolution.

Condoluci, M., Mahmoodi, T., 2018. Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges. Comput. Netw. 146, 65–84.

Dahlman, E., Parkvall, S., Skold, J., 2013. 4G: LTE/LTE-Advanced for Mobile Broadband. Academic Press.

Desai, S.K., Dua, A., Kumar, N., Das, A.K., Rodrigues, J.J., 2020. Cache poisoning prevention scheme in 5G-enabled vehicular networks: A tangle-based theoretical perspective. In: 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC). IEEE, pp. 1–6.

Dey, S., 2018. Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work. In: 2018 10th Computer Science and Electronic Engineering (CEEC). IEEE, pp. 7–10.

Dik, D., Berger, M.S., 2021. Transport security considerations for the open-RAN fronthaul. In: 2021 IEEE 4th 5G World Forum (5GWF). IEEE, pp. 253–258.

Docomo, N., 2021. 5G Open RAN Ecosystem Whitepaper. Whitepaper, p. 31, doi:https://www.nttdocomo.co.jp/binary/pdf/corporate/technology/whitepaper_5g_open_ran/OREC_WP.pdf.

Dolatshahi, S., Polak, A., Goeckel, D.L., 2010. Identification of wireless users via power amplifier imperfections. In: 2010 Conference Record of the Forty Fourth Asilomar Conference on Signals, Systems and Computers. pp. 1553–1557.

Dong, Z., Kane, K., Camp, L.J., 2016. Detection of rogue certificates from trusted certificate authorities using deep neural networks. ACM Trans. Priv. Secur. 19 (2), 1–31.

Doshi, R., Apthorpe, N., Feamster, N., 2018. Machine learning DDoS detection for consumer internet of things devices. In: 2018 IEEE Security and Privacy Workshops (SPW). IEEE, pp. 29–35.

Dryjański, M., Kułacz, Ł., Kliks, A., 2021. Toward modular and flexible open RAN implementations in 6G networks: Traffic steering use case and O-RAN xapps. Sensors 21 (24), 8173.

Dutta, B., Krichel, A., Odini, M.-P., 2021. The challenge of zero touch and explainable AI. J. ICT Stand. 147–158.

Eric Wenger, C., 2020. Security in open RAN networks, blog, industry. p. 7, doi:https://blogs.cisco.com/gov/security-in-open-ran-networks.

Ericsson, 2020. Security Considerations of Open-RAN. White Paper, doi:https://www.ericsson.com/4a4b77/assets/local/security/security-considerations-open-ran.pdf.

Faulhaber, G.R., Farber, D.J., 2003. Spectrum management: Property rights, markets, and the commons. In: Rethinking Rights and Regulations: Institutional Responses To New Communication Technologies. MIT Press Cambridge, MA, pp. 193–226.

Ferrag, M.A., Maglaras, L., Argyriou, A., Kosmanos, D., Janicke, H., 2018. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. J. Netw. Comput. Appl. 101, 55–82.

Fetterolf, P., 2021. The economic benefits of open RAN technology. URL https://infohub.delltechnologies.com/section-assets/acg-the-economic-benefits-of-open-ran-technology.

Floridi, L., 2021. Digital time: latency, real-time, and the onlife experience of everyday time. Philos. Technol. 34 (3), 407–412.

Gabilondo, Á., Fernández, Z., Martín, Á., Angueira, P., Montalbán, J., 2022. VNF lifecycle evaluation study for virtualized feMBMS. In: 2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). IEEE, pp. 238–242.

Garcia-Saavedra, A., Costa-Perez, X., 2021. O-RAN: Disrupting the virtualized RAN ecosystem. IEEE Commun. Stand. Mag..

Gavrilovska, L., Rakovic, V., Denkovski, D., 2020. From cloud RAN to open RAN. Wirel. Pers. Commun. 113 (3), 1523–1539.

Ge, M., Hong, J.B., Guttmann, W., Kim, D.S., 2017. A framework for automating security analysis of the internet of things. J. Netw. Comput. Appl. 83, 12–27.

George, G., Kotey, J., Ripley, M., Sultana, K.Z., Codabux, Z., 2021. A preliminary study on common programming mistakes that lead to buffer overflow vulnerability. In: 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, pp. 1375–1380.

Gindraux, S., 2002. From 2G to 3G: A guide to mobile security. In: Third International Conference on 3G Mobile Communication Technologies. IET, pp. 308–311.

Goodfellow, I., Papernot, N., Huang, S., Duan, Y., Abbeel, P., Clark, J., 2017. Attacking machine learning with adversarial examples, vol. 24.

Hanselman, E., 2020. Security benefits of open virtualized RAN. p. 13, doi:https://www.redhat.com/cms/managed-files/ve-451-research-telco-vran-security-analyst-material-f23695-en.pdf.

Harer, J.A., Kim, L.Y., Russell, R.L., Ozdemir, O., Kosta, L.R., Rangamani, A., Hamilton, L.H., Centeno, G.I., Key, J.R., Ellingwood, P.M., et al., 2018. Automated software vulnerability detection with machine learning. arXiv preprint arXiv:1803.04497.

Hassija, V., Chamola, V., Gupta, V., Jain, S., Guizani, N., 2020. A survey on supply chain security: Application areas, security threats, and solution architectures. IEEE Internet Things J. 8 (8), 6222–6246.

He, L., Yan, Z., Atiquzzaman, M., 2018. LTE/LTE-A network security data collection and analysis for security measurement: A survey. IEEE Access 6, 4220–4242.

Hewa, T., Bracken, A., Ylianttila, M., Liyanage, M., 2020. Blockchain-based automated certificate revocation for 5G IoT. In: ICC 2020 - 2020 IEEE International Conference on Communications (ICC). pp. 1–7.

Hewa, T.M., Braeken, A., Liyanage, M., Ylianttila, M., 2022. Fog computing and blockchain based security service architecture for 5G industrial IoT enabled cloud manufacturing. IEEE Trans. Ind. Inform. 1.

Hossain, M.F., Mahin, A.U., Debnath, T., Mosharrof, F.B., Islam, K.Z., 2019. Recent research in cloud radio access network (C-RAN) for 5G cellular systems-A survey. J. Netw. Comput. Appl. 139, 31–48.

Hsu, T.H.-C., 2018. Hands-on Security in DevOps: Ensure Continuous Security, Deployment, and Delivery with DevSecOps. Packt Publishing Ltd.

Hu, H., Salcic, Z., Sun, L., Dobbie, G., Yu, P.S., Zhang, X., 2021. Membership inference attacks on machine learning: A survey. ACM Comput. Surv..

Illiano, V.P., Lupu, E.C., 2015. Detecting malicious data injections in wireless sensor networks: A survey. ACM Comput. Surv. 48 (2), 1–33.

Iturria-Rivera, P.E., Zhang, H., Zhou, H., Mollahasani, S., Erol-Kantarci, M., 2022. Multi-agent team learning in virtualized open radio access networks (o-RAN). Sensors 22 (14), 5375.

Jarraya, Y., Eghtesadi, A., Sadri, S., Debbabi, M., Pourzandi, M., 2015. Verification of firewall reconfiguration for virtual machines migrations in the cloud. Comput. Netw. 93, 480–491.

Jian, T., Rendon, B.C., Ojuba, E., Soltani, N., Wang, Z., Sankhe, K., Gritsenko, A., Dy, J., Chowdhury, K., Ioannidis, S., 2020. Deep learning for RF fingerprinting: A massive experimental study. IEEE Internet Things Mag. 3 (1), 50–57.

Johnson, C.D., 2020. Open ran policy coalition comment for national strategy for secure 5g. URL https://www.cnas.org/publications/reports/open-future.

Johnson, D., Maas, D., Van Der Merwe, J., 2022. NexRAN: Closed-loop RAN slicing in POWDER-A top-to-bottom open-source open-RAN use case. In: Proceedings of the 15th ACM Workshop on Wireless Network Testbeds, Experimental Evaluation & CHaracterization. pp. 17–23.

Jones, D., Snider, C., Nassehi, A., Yon, J., Hicks, B., 2020. Characterising the Digital Twin: A systematic literature review. CIRP J. Manuf. Sci. Technol. 29, 36–52.

Jurcut, A., Niculcea, T., Ranaweera, P., Le-Khac, N.-A., 2020. Security considerations for Internet of Things: A survey. SN Comput. Sci. 1 (4), 1–19.

Kapetanovic, D., Zheng, G., Rusek, F., 2015. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. IEEE Commun. Mag. 53 (6), 21–27.

Kawahara, S.A.T., Matsukawa, A.U.R., 2019. O-RAN alliance standardization trends.

Kawashima, R., 2021. A vision to software-centric cloud native network functions: Achievements and challenges. In: 2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR). IEEE, pp. 1–7.

Kazemifard, N., Shah-Mansouri, V., 2021. Minimum delay function placement and resource allocation for Open RAN (O-RAN) 5G networks. Comput. Netw. 188, 107809.

Khan, R., Kumar, P., Jayakody, D.N.K., Liyanage, M., 2020. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. IEEE Commun. Surv. Tutor. 22 (1), 196–248.

Klement, F., Katzenbeisser, S., Ulitzsch, V., Krämer, J., Stanczak, S., Utkovski, Z., Bjelakovic, I., Wunder, G., 2022. Open or not open: Are conventional radio access networks more secure and trustworthy than Open-RAN? arXiv preprint arXiv:2204.12227.

Lal, S., Taleb, T., Dutta, A., 2017. NFV: Security threats and best practices. IEEE Commun. Mag. 55 (8), 211–217.

Larsson, E.G., Edfors, O., Tufvesson, F., Marzetta, T.L., 2014. Massive MIMO for next generation wireless systems. IEEE Commun. Mag. 52 (2), 186–195.

Lee, L.-H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., Kumar, A., Bermejo, C., Hui, P., 2021a. All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. arXiv preprint arXiv:2110.05352.

Lee, H., Jang, Y., Song, J., Yeon, H., 2021b. O-RAN AI/ML workflow implementation of personalized network optimization via reinforcement learning. In: 2021 IEEE Globecom Workshops (GC Wkshps). IEEE, pp. 1–6.

Lee, Y., Moon, C., Ko, H., Lee, S.-H., Yoo, B., 2020. Unified representation for XR content and its rendering method. In: The 25th International Conference on 3D Web Technology. pp. 1–10.

Lee-Makiyama, H., 2020. Open RAN: The technology, its politics and Europe's response. doi:https://ecipe.org/wp-content/uploads/2020/10/ECI_20_PolicyBrief_08_2020_LY03.pdf.

Li, Y., Jiang, Y., Li, Z., Xia, S.-T., 2022. Backdoor learning: A survey. IEEE Trans. Neural Netw. Learn. Syst. 1–18. http://dx.doi.org/10.1109/TNNLS.2022.3182979.

Lichtman, M., Rao, R., Marojevic, V., Reed, J., Jover, R.P., 2018. 5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation. In: 2018 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, pp. 1–6.

Ling, X., Wang, J., Bouchoucha, T., Levy, B.C., Ding, Z., 2019. Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm. IEEE Access 7, 9714–9723.

Lipton, A., Treccani, A., 2021. Blockchain and Distributed Ledgers: Mathematics, Technology, and Economics. World Scientific.

Liu, Y., Ning, P., Dai, H., 2010. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. In: 2010 IEEE Symposium on Security and Privacy. IEEE, pp. 286–301.

Liyanage, M., Pham, Q.-V., Dev, K., Bhattacharya, S., Maddikunta, P.K.R., Gadekallu, T.R., Yenduri, G., 2022. A survey on Zero touch network and Service (ZSM) Management for 5G and beyond networks. J. Netw. Comput. Appl. 103362. http://dx.doi.org/10.1016/j.jnca.2022.103362, URL https://www.sciencedirect.com/science/article/pii/S1084804522000297.

Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., Ylianttila, M., 2018. 5G privacy: Scenarios and solutions. In: 2018 IEEE 5G World Forum (5GWF). pp. 197–203.

Mantas, G., Komninos, N., Rodriuez, J., Logota, E., Marques, H., 2015. Security for 5G communications.

Mariniello, M., 2011. Fair, Reasonable and Non-Discriminatory (FRAND) terms: a challenge for competition authorities. J. Compet. Law Econ. 7 (3), 523–541.

Masur, P.H., Reed, J.H., Tripathi, N., 2022. Artificial intelligence in open-radio access network. IEEE Aerosp. Electron. Syst. Mag. 1–11. http://dx.doi.org/10.1109/MAES.2022.3186966.

Michael Veale, R.B., Edwards, L., 2018. Algorithms that remember: model inversion attacks and data protection law. Philos. Trans. R. Soc. A.

Mimran, D., Bitton, R., Kfir, Y., Klevansky, E., Brodt, O., Lehmann, H., Elovici, Y., Shabtai, A., 2022. Evaluating the security of open radio access networks. arXiv preprint arXiv:2201.06080.

Mitchell, G., 2021. Openran is open for debate, Mpirical. doi:https://www.mpirical.com/blog/open-ran-is-open-for-debate.

Morais, F.Z., da Costa, C.A., Alberti, A.M., Both, C.B., da Rosa Righi, R., 2020. When SDN meets C-RAN: A survey exploring multi-point coordination, interference, and performance. J. Netw. Comput. Appl. 162, 102655.

Moreira, C.M., Kaddoum, G., Baek, J.-Y., Selim, B., 2021. Task allocation framework for software-defined fog v-RAN. IEEE Internet Things J. 8 (18), 14187–14201.

Needham, R.M., 1993. Denial of service. In: Proceedings of the 1st ACM Conference on Computer and Communications Security. pp. 151–153.

Nguyen, K., Le Nguyen, P., Li, Z., Sekiya, H., 2021. Empowering 5G mobile devices with network softwarization. IEEE Trans. Netw. Serv. Manag. 18 (3), 2492–2501.

Niknam, S., Roy, A., Dhillon, H.S., Singh, S., Banerji, R., Reed, J.H., Saxena, N., Yoon, S., 2020. Intelligent O-RAN for beyond 5G and 6G wireless networks. arXiv preprint arXiv:2005.08374.

Nolle, T., 2020. Is Ericsson Right About Open RAN Security?. Blog, doi:https://blog.cimicorp.com/?p=4289.

O-Ran Alliance Security Focus Group, 2021a. O-RAN Security Threat Modeling and Remediation Analysis, O-RAN.WG1.SFG.Threat-Model-V01.00. Technical Specifications, p. 57.

O-Ran Alliance Security Focus Group, 2021b. O-RAN Security Requirement Specifications. O-RAN.SFG.Security-Requirements-Specifications-V02.00, p. 45.

O-Ran Policy Coalition, 2021. Open-RAN security in 5G. doi:https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf.

O'Dea, S., 2021. Number of mobile subscriptions worldwide 1993–2021. URL https://www.statista.com/statistics/262950/global-mobile-subscriptions-since-1993/.

Orhan, O., Swamy, V.N., Tetzlaff, T., Nassar, M., Nikopour, H., Talwar, S., 2021. Connection management xAPP for O-RAN RIC: A graph neural network and reinforcement learning approach. In: 2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE, pp. 936–941.

Palmbach, D., Breitinger, F., 2020. Artifacts for detecting timestamp manipulation in NTFS on windows and their reliability. Forensic Sci. Int.: Digit. Investig. 32, 300920.

Parvez, I., Rahmati, A., Guvenc, I., Sarwat, A.I., Dai, H., 2018. A survey on low latency towards 5G: RAN, core network and caching solutions. IEEE Commun. Surv. Tutor. 20 (4), 3098–3130.

Polese, M., Bonati, L., D'Oro, S., Basagni, S., Melodia, T., 2022. Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges. arXiv preprint arXiv:2202.01032.

Qiang, W., Yang, J., Jin, H., Shi, X., 2018. PrivGuard: Protecting sensitive kernel data from privilege escalation attacks. IEEE Access 6, 46584–46594.

Ramezanpour, K., Jagannath, J., 2021. Intelligent zero trust architecture for 5G/6G tactical networks: Principles, challenges, and the role of machine learning. arXiv preprint arXiv:2105.01478.

2022. "O-RAN alliance". URL https://www.o-ran.org/.

Ranaweera, P., de Alwis, C., Jurcut, A.D., Liyanage, M., 2022. Realizing contact-less applications with Multi-Access Edge Computing. ICT Express.

Ranaweera, P., Imrith, V.N., Liyanag, M., Jurcut, A.D., 2020. Security as a service platform leveraging multi-access edge computing infrastructure provisions. In: ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, pp. 1–6.

Ranaweera, P., Jurcut, A.D., Liyanage, M., 2021. Survey on multi-access edge computing security and privacy. IEEE Commun. Surv. Tutor. 23 (2), 1078–1124.

Rasser, M., Riikonen, A., 2020. Open future the way forward on 5G. URL https://www.cnas.org/publications/reports/open-future.

Redhat, 2020. The inherent security of Open RAN. Fierce Wireless, doi:https://www.fiercewireless.com/sponsored/inherent-security-open-ran.

Reus-Muns, G., Jaisinghani, D., Sankhe, K., Chowdhury, K.R., 2020. Trust in 5G open RANs through machine learning: RF fingerprinting on the POWDER PAWR platform. In: GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, pp. 1–6.

Rose, S., Borchert, O., Mitchell, S., Connelly, S., 2020. Zero Trust Architecture. Tech. rep, National Institute of Standards and Technology.

Salahuddin, M.A., Pourahmadi, V., Alameddine, H.A., Bari, M.F., Boutaba, R., 2021. Chronos: DDoS attack detection using time-based autoencoder. IEEE Trans. Netw. Serv. Manag..

Sasaki, T., Karino, S., Tani, M., Nakajima, K., Tomita, K., Yamagaki, N., 2020. Security architecture for trustworthy systems in 5g era. arXiv preprint arXiv:2007.14756.

Schaefer, R.F., Amarasuriya, G., Poor, H.V., 2017. Physical layer security in massive MIMO systems. In: 2017 51st Asilomar Conference on Signals, Systems, and Computers. pp. 3–8.

Sevinç, P.E., Strasser, M., Basin, D., 2007. Securing the distribution and storage of secrets with trusted platform modules. In: IFIP International Workshop on Information Security Theory and Practices. Springer, pp. 53–66.

Sharafaldin, I., Lashkari, A.H., Hakak, S., Ghorbani, A.A., 2019. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In: 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, pp. 1–8.

Shi, Y., Sagduyu, Y.E., 2021. Adversarial machine learning for flooding attacks on 5G radio access network slicing. In: 2021 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, pp. 1–6.

Singh, S.K., Singh, R., Kumbhani, B., 2020. The evolution of radio access network towards open-RAN: Challenges and opportunities. In: 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). pp. 1–6.

Siriwardhana, Y., Porambage, P., Liyanage, M., Ylianttila, M., 2021. AI and 6G security: Opportunities and Challenges. In: 2021 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit). pp. 616–621.

Software org, B.F., 2021. How open RAN technologies will lead to secure, innovative 5G networks. doi:https://software.org/reports/how-open-ran-technologies-will-lead-secure-innovative-5g-networks/.

Soldani, D., 2019. 5G and the future of security in ICT. In: 2019 29th International Telecommunication Networks and Applications Conference (ITNAC). IEEE, pp. 1–8.

Soltanieh, N., Norouzi, Y., Yang, Y., Karmakar, N.C., 2020. A review of radio frequency fingerprinting techniques. IEEE J. Radio Freq. Identif. 4 (3), 222–233.

Sorensen, L.T., Khajuria, S., Skouby, K.E., 2015. 5G visions of user privacy. In: 2015 IEEE 81st Vehicular Technology Conference (VTC Spring). IEEE, pp. 1–4.

Spremić, M., Šimunic, A., 2018. Cyber security challenges in digital economy. In: Proceedings of the World Congress on Engineering, Vol. 1. International Association of Engineers Hong Kong, China, pp. 341–346.

Sun, G., Cong, Y., Dong, J., Wang, Q., Lyu, L., Liu, J., 2021. Data poisoning attacks on federated machine learning. IEEE Internet Things J..

Tamim, I., Saci, A., Jammal, M., Shami, A., 2021. Downtime-aware O-RAN VNF deployment strategy for optimized self-healing in the O-cloud. In: 2021 IEEE Global Communications Conference (GLOBECOM). pp. 1–6. http://dx.doi.org/10.1109/GLOBECOM46510.2021.9685775.

Tanakas, P., Ilias, A., Polemi, N., 2021. A novel system for detecting and preventing SQL injection and cross-site-script. In: 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET). IEEE, pp. 1–6.

Tataria, H., Shafi, M., Molisch, A.F., Dohler, M., Sjöland, H., Tufvesson, F., 2021. 6G wireless systems: Vision, requirements, challenges, insights, and opportunities. Proc. IEEE 109 (7), 1166–1199.

Tian, F., Zhang, P., Yan, Z., 2017. A survey on C-RAN security. IEEE Access 5, 13372–13386.

2022. "The telecom infra project (TIP)". URL https://telecominfraproject.com/openran/.

Umesh, A., Teshima, K., 2020. O-RAN Alliance trends and NTT DOCOMO's activities. IEICE Tech. Rep. 120 (29), 29.

ur Rehman, M.H., Salah, K., Damiani, E., Svetinovic, D., 2019. Trust in blockchain cryptocurrency ecosystem. IEEE Trans. Eng. Manage. 67 (4), 1196–1212.

van der Merwe, J.R., Zubizarreta, X., Lukčin, I., Rügamer, A., Felber, W., 2018. Classification of spoofing attack types. In: 2018 European Navigation Conference (ENC). IEEE, pp. 91–99.

Varga, P.J., Nádai, L., Tóth, A.B., Kail, E., Wührl, T., Gyányi, S., Kún, G., Kovács, R., Bánáti, A., Kozlovszky, M., 2022. 5G RAN research in Óbuda University. In: 2022 IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics (SAMI). IEEE, pp. 000359–000366.

Velliangiri, S., Manoharn, R., Ramachandran, S., Rajasekar, V.R., 2021. Blockchain based privacy preserving framework for emerging 6G wireless communications. IEEE Trans. Ind. Inform..

Verizon, 2021. How and Why Private 5G Networks are Taking Flight, Addressing the Need for Enterprise Network Security, Speed and Bandwidth in the U.S.. News Center, doi:https://www.verizon.com/about/news/how-and-why-private-5g-networks.

Wang, T.-H., Chen, Y.-C., Huang, S.-J., Hsu, K.-S., Hu, C.-H., 2021. Design of a network management system for 5G open RAN. In: Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, pp. 138–141.

Wang, Y., Jere, S., Banerjee, S., Liu, L., Shetty, S., Dayekh, S., 2022. Anonymous jamming detection in 5G with Bayesian network model based inference analysis. In: 2022 IEEE 23rd International Conference on High Performance Switching and Routing (HPSR). IEEE, pp. 151–156.

Weissberger, A., 2021. Strand consult: The 10 parameters of open RAN; AT&T memo to FCC. In: IEEE ComSoc, Technology Blog. doi:https://techblog.comsoc.org/2021/05/01/strand-consult-the-10-parameters-of-open-ran-att-memo-to-fcc/.

Wood, A.D., Stankovic, J.A., 2004. A taxonomy for denial-of-service attacks in wireless sensor networks. In: Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, Vol. 4. Citeseer, pp. 739–763.

Wright, M., Adler, M., Levine, B.N., Shields, C., 2003. Defending anonymous communications against passive logging attacks. In: 2003 Symposium on Security and Privacy, 2003. IEEE, pp. 28–41.

Wypiór, D., Klinkowski, M., Michalski, I., 2022. Open RAN-radio access network evolution, benefits and market trends. Appl. Sci. 12 (1), 408.

Xiao, Z., Xiao, Y., 2012. Security and privacy in cloud computing. IEEE Commun. Surv. Tutor. 15 (2), 843–859.

Xu, H., Zhang, L., Sun, Y., et al., 2021. BE-RAN: Blockchain-enabled open RAN with decentralized identity management and privacy-preserving communication. arXiv preprint arXiv:2101.10856.

Yadav, R.B., Kumar, P.S., Dhavale, S.V., 2020. A survey on log anomaly detection using deep learning. In: 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO). IEEE, pp. 1215–1220.

Yampolskiy, R.V., 2020. Unexplainability and incomprehensibility of AI. J. Artif. Intell. Conscious. 7 (02), 277–291.

Yang, W., Fung, C., 2016. A survey on security in network functions virtualization. In: IEEE NetSoft Conference and Workshops (NetSoft). pp. 15–19.

Yang, M., Li, Y., Jin, D., Su, L., Ma, S., Zeng, L., 2013. OpenRAN: A software-defined RAN architecture via virtualization. ACM SIGCOMM Comput. Commun. Rev. 43 (4), 549–550.
Youssef, K., Bouchard, L., Haigh, K., Silovsky, J., Thapa, B., Valk, C.V., 2018. Machine learning approach to RF transmitter identification. IEEE J. Radio Freq. Identif. 2 (4), 197–205.
Ziegler, V., Yrjölä, S., 2021. How to make 6G a general purpose technology: Prerequisites and value creation paradigm shift. In: 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). IEEE, pp. 586–591.

Madhusanka Liyanage is an Assistant Professor/Ad Astra Fellow and Director of Graduate Research at the School of Computer Science, University College Dublin, Ireland. He is also acting as a Docent/Adjunct Professor at the Center for Wireless Communications, University of Oulu, Finland, and Honorary Adjunct Professor of Network Security, The Department of Electrical and Information Engineering, University of Ruhuna, Sri Lanka. He received his B.Sc. degree (First Class Honors) in electronics and telecommunication engineering from the University of Moratuwa, Moratuwa, Sri Lanka, in 2009, the M.Eng. degree from the Asian Institute of Technology, Bangkok, Thailand, in 2011, the M.Sc. degree from the University of Nice Sophia Antipolis, Nice, France, in 2011, and the Doctor of Technology degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. From 2011 to 2012, he worked as a Research Scientist at the I3S Laboratory and Inria, Sophia Antipolis, France. He was also a recipient of the prestigious Marie Skłodowska-Curie Actions Individual Fellowship and Government of Ireland Postdoctoral Fellowship during 2018-2020. During 2015-2018, he has been a Visiting Research Fellow at the CSIRO, Australia, the Infolabs21, Lancaster University, U.K., Computer Science and Engineering, The University of New South Wales, Australia, School of IT, University of Sydney, Australia, LIP6, Sorbonne University, France and Computer Science and Engineering, The University of Oxford, U.K. He is also a senior member of IEEE. In 2020, he received the "2020 IEEE ComSoc Outstanding Young Researcher" award by IEEE ComSoc EMEA. In 2021, he was ranked among the World's Top 2 Scientists (2020) in the List prepared by Elsevier BV, Stanford University, USA. Also, he was awarded an Irish Research Council (IRC) Research Ally Prize as part of the IRC Researcher of the Year 2021 awards for the positive impact he has made as a supervisor. He is also currently an expert consultant at European Union Agency for Cybersecurity (ENISA). In 2021, Liyanage was elevated as Funded Investigator of Science Foundation Ireland CONNECT Research Centre, Ireland. Moreover, he is an expert reviewer at different funding agencies in France, Qatar, UAE, Sri Lanka, and Kazakhstan. Dr. Liyanage's research interests are 5G/6G, SDN, IoT, Blockchain, MEC, mobile and virtual network security. More info: www.madhusanka.com.

An Braeken obtained her M.Sc. Degree in Mathematics from the University of Gent in 2002. In 2006, she received her Ph.D. in engineering sciences from the KU Leuven at the research group COSIC (Computer Security and Industrial Cryptography). She became professor in 2007 at the Erasmushoge school Brussel (currently since 2013, Vrije Universiteit Brussel) in the Industrial Sciences Department. Prior to joining the Erasmushoge school Brussel, she worked for almost 2 years at the management consulting company Boston Consulting Group (BCG). Her current interests include security and privacy protocols for IoT, cloud and fog, blockchain and 5G security. She is (co-)author of over 200 publications. She has been member of the program committee for numerous conferences and workshops and member of the editorial board for Security and Communications magazine. In addition, she is since 2014 expert reviewer for several EU calls. She has cooperated and coordinated more than 15 national and international projects.

Shahriar Shahabuddin is a signal processing specialist at the Mobile Networks organization of Nokia, Dallas, TX, USA. He also holds the position of Adjunct Professor at the University of Oulu, Finland. His research interests include VLSI signal processing, machine learning and physical layer security. He is a co-author of more than 40 scientific publications. He is a member of IEEE COMSOC and IEEE CAS societies.

Pasika Ranaweera (Member, IEEE) is working as a post-doctoral researcher at School of Computer Science, University College Dublin (UCD), Ireland; attached to the CONFIDENTIAL-6G project (EUC ID:101096435). He obtained his Bachelor Degree in Electrical and Information Engineering in 2010 from University of Ruhuna, Sri Lanka, received the Lanekassen scholarship for pursuing the Master's Degree in ICT in 2013 from University of Agder, Norway, and Ph.D. in Computer Science from UCD, Ireland in 2023. He was working on MEC edge computing paradigm security during his Ph.D., while focusing on service migration aspect. At the moment, Pasika is focused on security, privacy and trust issues in the Federated Learning domain and looking towards Blockchain as a viable solution. His additional research directives extend to the areas of lightweight security protocols, 5G and MEC integration technologies (SDN, NFV, Blockchain), security optimization, privacy preservation techniques and IoT security. He serves as a reviewer for IEEE IoT journal, IEEE IoT Magazine, IEEE TETC, SN Computer Science, and various IEEE hosted conferences and workshops under IEEE Communication Society (also a member of IEEE ComSoc). More info: https://ucdcs-research.ucd.ie/phd-student/pasika-sashmalranaweera/.