IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 8 March 2024, accepted 16 May 2024, date of publication 3 June 2024, date of current version 1 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3408690

SURVEY

A Survey for Intrusion Detection Systems in Open RAN

EMMANUEL N. AMACHAGHI[1], (Graduate Student Member, IEEE), MOHAMMAD SHOJAFAR[1], (Senior Member, IEEE), CHUAN HENG FOH[1], (Senior Member, IEEE), AND KLAUS MOESSNER[2], (Senior Member, IEEE)

[1]5G/6G Innovation Centre, Institute for Communication Systems, University of Surrey, GU2 7XH Surrey, U.K.
[2]Department of Communications Engineering, Chemnitz University of Technology, 09111 Chemnitz, Germany

Corresponding author: Emmanuel N. Amachaghi (e.amachaghi@surrey.ac.uk)

This work was supported by the U.K. Department for Science, Innovation, and Technology, under Project 5G Mobile open Radio Access Network (oRAN) for highly Dense Environments (MoDE).

ABSTRACT Open Radio Access Network (RAN) introduces a groundbreaking industry standard for Radio Access Networks, fostering vendor interoperability and network flexibility through open interfaces while leveraging network softwarization, Artificial, and Machine Learning Intelligence; however, it also poses significant security challenges due to its unique configuration, prompting stakeholders to cautiously approach its deployment and necessitating thorough analysis and implementation of security measures and standards. This paper systematically examines existing literature and case studies to underscore the indispensable role of Intrusion Detection Systems (IDS) in identifying and mitigating security breaches within Open RAN environments. We elucidate the distinct challenges that Open RAN's disaggregated architecture introduced and classify them into technical and non-technical threats. Finally, we discussed a series of new advancements gaining momentum in the Open RAN security domain and provided insights for future research directions.

INDEX TERMS Future mobile networks, intrusion detection systems (IDS), open radio access networks (RAN), resource allocation, security.

I. INTRODUCTION

Mobile networks comprise of *two* key domains - the *Core Network* and *Radio Access Network (RAN)*. Both parts have seen great step-changes from 1st to 5th generation, leading beyond 5th generation (B5G) and 6th generation. The interfaces within the core have seen a greater deal of standardization by 3GPP, ETSI and ITU. This is a testament to the fact that today, operators' choice of network deployment is one with multiple vendors to de-risk a well-known term called *vendor lock-in*. However, RAN deployment has been monolithic and closed, with a single vendor supplying RAN elements. Recently, there has been some development in the RAN technology, which has been harvested into the Open RAN. Open RAN is a revolutionary architectural framework for mobile and wireless communication networks, designed to provide greater flexibility, interoperability, and cost-efficiency by disaggregating (making interfaces 'Open') and virtualizing various network components [1]. It aims to break away from the traditional and vendor-locked RAN architectures, promoting vendor diversity. Open RAN architecture has gained popularity in the telecommunications industry due to its potential for cost reduction, interoperability, and flexibility. Open RAN offers several benefits, including complete visibility, selection of best modules, diversity, and modularity [2]. Open RAN integrates the benefits and advancements of network softwarization, Artificial Intelligence, and Machine Learning (AI/ML) to enhance the operation of RAN. AI helps overcome various challenges of 6G Open RANs via intelligent and data-driven solutions that can be applied to the components of the Open RAN architecture. Open RAN technology provides multiple advantages over conventional, legacy, and proprietary RAN systems, including enhanced network performance, cost-efficiency, reduced waste of wireless infrastructure and spectrum resources, streamlined, automated operational

The associate editor coordinating the review of this manuscript and approving it for publication was Tawfik Al-Hadhrami.

network functions, and the ability to upgrade or replace specific components without affecting the entire network. In [3], Ahmad et al. detailed an overview of security challenges and solutions in 5G technologies, including cloud computing, Software Defined Networks (SDN), and Network Function Virtualization (NFV), while addressing user privacy concerns in 5G systems. They emphasize the need for timely security measures to address forefront security challenges in 5G. The paper explores various security threats to the back-end platform and network-based mobile security threats targeting Radio Access Technologies (RATs). These threats encompass data replication, HTTP and XML DoS attacks, WiFi sniffing, address impersonation, and session hijacking. To extend this, decentralization and virtualization aspects of Open RAN introduce unique security challenges. Anomaly detection and IDS are critical components [4], [5], [6], [7], for securing Open RAN networks, as they can help identify and respond to potential security threats as traditional firewalls or Security Information and Event Management (SIEM) tools cannot provide sufficient security required [8]. This survey paper delves into the world of IDS, particularly in the context of Open-RAN, to provide a comprehensive overview of the current state of research and practice.

In traditional RAN, there is close collaboration between RAN vendors to guarantee compatibility. However, the downside of this cooperative model is that it introduces complexity in interoperability, which may hinder innovation [9]. Open RAN comes in to address this flippancy by introducing RAN disaggregation. Open-RAN allows network operators to choose components from multiple vendors in this open model, promoting vendor diversity. However, this also presents the challenge of ensuring the security of these diverse components, such as Radio Units (RUs), Distributed Units (DUs), and Centralized Units (CUs), which can come from multiple vendors with varying security practices and standards. Ensuring seamless interoperability and integration of these components can be complex as incompatibilities or misconfigurations can create security gaps, making the network susceptible to vulnerabilities and attacks [10]. This could lead to supply chain risk with chances of introducing backdoors, malware, or other vulnerabilities, allowing unauthorized access to the network. Vendors release security patches and updates at different intervals, hence various security policies and mechanisms with inconsistencies in security policies that can create gaps, making it difficult to enforce a unified security strategy. On the one hand, coordinating and applying these patches across a multi-vendor environment can be complex and time-consuming, and delayed or incomplete patching can leave the network exposed to known vulnerabilities, making it an attractive target for attackers on the other hand.

Security in the context of Open-RAN is not a one-time endeavor but a continuous, evolving process. Constant monitoring and real-time auditing of open interfaces constitute vital components of a comprehensive security strategy. Continuous monitoring ensures the prompt detection of anomalous activities, unauthorized access attempts, or other potential security breaches using IDS.

A. MOTIVATION

The significance of integrating security into an architecture from the outset cannot be overstated in a rapidly evolving digital environment. Secure systems play a multifaceted role in ensuring the success and widespread adoption of transformative network architectures like O-RAN, safeguarding sensitive data and communications. As O-RAN deployment gains momentum, robust security frameworks, including IDS, become increasingly crucial to mitigate evolving cyber threats and vulnerabilities introduced by its disaggregated architecture. Therefore, by synthesizing current research, our survey aims to offer a holistic understanding of the security landscape surrounding Open RAN deployments and emphasize on the critical need to consolidate existing knowledge, discern emerging threats, and propose effective mitigation strategies. Also, as Open RAN gains momentum in academic and industry domains, deepening our comprehension of its security implications is imperative. Our survey endeavors to catalyze further research and development in this vital domain by shedding light on the distinctive security challenges inherent in O-RAN architectures.

B. OUR CONTRIBUTION

Our contribution to the literature on Open RAN security encapsulates several pivotal dimensions:

- **Comprehensive Overview of Open RAN security:** We present a meticulous survey of both published works and ongoing research endeavors concerning the security facets of Open RAN. This thoroughly examines the distinct security challenges inherent to this burgeoning architecture.
- **Open RAN Security Taxonomy:** We introduce a structured taxonomy delineating the diverse security threats confronting Open RAN networks. Categorized into technical and non-technical threats, our taxonomy elucidates the potential impacts of these threats and offers insights into plausible mitigation strategies.
- **Intrusion Detection Systems (IDS) Review:** We conduct an in-depth analysis of IDS tailored for Open RAN environments. Our review explores the role of IDS in monitoring and responding to the evolving spectrum of threats and security issues within Open RAN networks.
- **Real-World Case Studies:** Drawing upon real-world deployments from early adopters, we provide detailed case studies elucidating how security is integrated into Open RAN deployment projects. These case studies offer tangible insights into the strategies employed by organizations to bolster security within their Open RAN ecosystems.

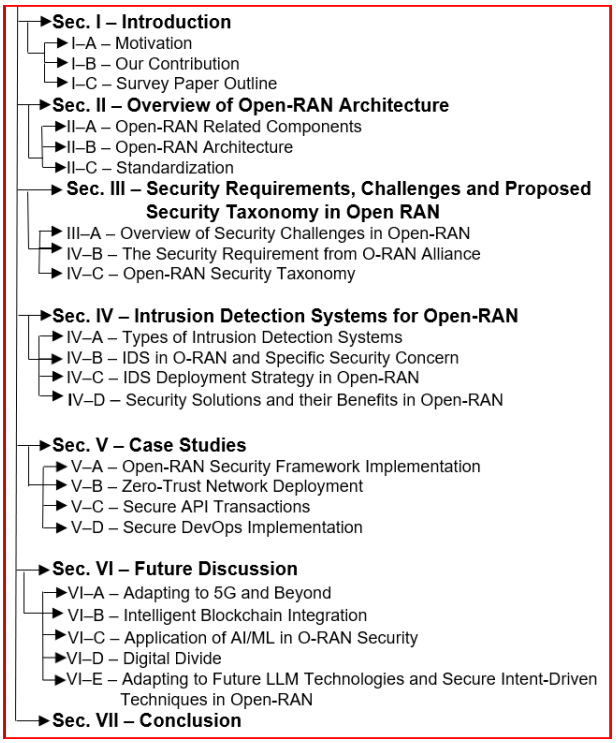


FIGURE 1. Overview of survey paper structure.

- **Emerging Security Technologies:** We spotlight emerging technologies with significant promise for enhancing security within the Open RAN ecosystem. By delineating these innovative solutions, we aim to provide researchers and industry stakeholders with valuable insights into avenues for advancing security in Open RAN networks.

C. SURVEY PAPER OUTLINE

The rest of this survey is organized as shown in Fig 1. In Section II, we presented an overview of Open RAN architecture. We looked at threat vectors, security risks and challenges in Section III and presented an intrusion detection system in Open RAN in Section IV. To provide our readers with a view of how the industry has embraced Open RAN architecture in Section V, we presented a deployment case study detailing the operator's real-world experience, and finally, we finished by providing future direction in Section VI and concluded in Section VII pronouncing the importance of advanced security measures and IDS to secure Open RAN.

II. OVERVIEW OF OPEN RAN ARCHITECTURE

This section presents the Open RAN structure, related engaged components, and standardization descriptions.

A. OPEN-RAN RELATED COMPONENTS

Open-RAN introduces the concept of open interfaces and standards, (open) Fronthaul and (open) Midhaul (for establishing connections between various sections of the RAN), (open) Backhaul (connects the RAN to the Core) [11], [12], [13]. These enable network operators to mix and match hardware and software components from different vendors, thereby fostering competition and innovation in the telecommunications industry. Open-RAN often incorporates virtualization technologies to run network functions and applications as virtualized instances. This allows for greater flexibility and scalability, promoting the use of open-source software and open standards, encouraging innovation and reducing vendor lock-in. Initiatives like the O-RAN Alliance work on defining open standards and specifications for Open-RAN architecture. The SDN principles are employed

TABLE 1. Summary of key acronyms used in this survey.

Acronym	Definition
3GPP	Third Generation Partnership Project
AI	Artificial Intelligence
API	Application Programming Interface
BBU	Based-Band Unit
BE-RAN	Blockchain Enabled-Radio Access Network
BS	Base Station
CI/CD	Continuous Improvement / Continuous Development
CP	Control Plane
CVD	Coordinated Vulnerability Disclosure
DDoS	Distributed Denial of Service
DTLS	Datagram Transport Layer Security
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
FFT	Fast Fourier Transform
FL	Federated Learning
IDS	Intrusion Detection System
IETF	The Internet Engineering Task Force
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
LLM	Large Language Model
ML	Machine Learning
MNO	Mobile Network Operator
MITM	Man-in-the-Middle
MTD	Moving Target Defense
NFV	Network Function Virtualization
NR	New Radio
N-RT RIC	Near-Real Time RAN Intelligent Network
Non-RT RIC	Non-Real Time RAN Intelligent Network
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Admin
O-CU-CP	O-RAN Central Unit–Control Plane
O-CU-UP	O-RAN Central Unit–User Plane
O-DU	O-RAN Distributed Unit
O-RU	O-RAN Radio Unit
P2P	Peer 2 Peer
QoS	Quality of Service
RAN	Radio Access Network
RIC	RAN Intelligent Controller
RRU	Remote Radio Unit
SDN	Software-Defined Networking
SIEM	Security Information and Event Management
SMO	Service Management and Orchestration
SDN	Software Defined Networking
SDO	Standard Development Organization
SFG	Security Focus Group
SSA	Signaling Storm Attack
TN	Transport Network
OSC	O-RAN Software Community
PDCP	Packet Data Convergence Protocol
RRC	Radio Resource Control
TIP	Telecom Infra Project
TLS	Transport Layer Security
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UP	User Plane
WG	Working Group
ZTA	Zero Trust Architecture

to dynamically configure, manage, and optimize network resources.

1) DECOUPLED COMPONENTS

O-RAN separates various network functions into modular and interoperable components. These include the Radio Unit (RU), Distributed Unit (DU), and Centralized Unit (CU). This decoupling allows network operators to choose different vendors for hardware and software, choose best-of-breed solutions and technologies such on-prem or cloud deployment, containerization and kubernetes, thereby enabling faster deployment of new technologies and innovative practices in network infrastructure. O-RAN relies on standardized, open interfaces between these components, facilitating a multi-vendor ecosystem characterized by healthy competition in quality [14].

2) VIRTUALIZATION AND SOFTWARE-DEFINED NETWORKING (SDN)

O-RAN leverages virtualization and SDN principles to enable dynamic network management and efficient resource allocation. It uses cloud-native technologies to run virtualized network functions and applications. Open-RAN systems often employ centralized orchestration and management, allowing network operators to control and optimize the entire network from a central location. This centralization facilitates resource allocation, load balancing, and dynamic configuration. The O-RAN ecosystem encourages these and the Open-source initiatives (the O-RAN Alliance) for the development of open standards and specifications.

3) FLEXIBILITY AND SCALABILITY

Network operators can adapt their networks to changing requirements quickly as O-RAN can accommodate various network generations, from 2G to 5G, and potentially beyond. This is evident in Open RAN functional splits as shown in Fig. 3. So, for the sake of performance optimization, Open RAN offers the option of integrating network functions at different places along the signal path [15]. Different generations of mobile networks consists of Baseband Units (BBU) situated at the telecommunication towers to demodulate radio frequency signals, converting signals into digital data streams for backhaul. However, by disaggregating BBU, RUs split into DUs and CU, operators are able to place these functions efficiently for optimal performance and support use cases with stringent latency and costs requirements, although with trade-off on fronthaul bandwidth [12]. This introduces flexibility in network deployment. There are eight recognized methods for functionally splitting the RAN, each proposing a division of processing tasks, allowing different parts of the protocol stack to operate on distinct hardware components. O-RAN advocates for the use of option 7-2, split which divides the physical layer (PHY) into a high-PHY and a low-PHY. In option 7.2, certain functions such as uplink (UL), fast fourier transform (FFT), digital beamforming (if applicable), and prefiltering (specifically for PRACH - Physical Random Access Channel) take place in the Radio Unit (RU) [16]. The remaining PHY processes are handled in the Distributed Unit (DU). For the downlink (DL), functions like inverse FFT (iFFT), precoding, and digital beamforming (if applicable) are executed in the RU, while the rest of the PHY processing is carried out in the DU. Split 7.2 objectives include minimizing transport bandwidth impact and maximizing virtualization in gNB CU and gNB DU, enabling cost-effective Remote Radio Unit (RRU) designs, eliminating performance loss compared to integrated solutions, removing limitations on receiver architecture, ensuring compatibility with NR without redesign, and offering increased scalability through a fixed-rate streaming interface and centralized scheduling, while supporting advanced signal processing like UL compression [17].

4) INTELLIGENT, DATA-DRIVEN CONTROL

O-RAN introduces RAN Intelligent Controllers (RICs) that perform management and control functions at near-real-time and non-real-time scales. These controllers leverage data-driven closed-loop control to optimize network performance and enable dynamic network function allocation [18], providing enhanced network efficiency and responsiveness. The RICs introduce programmable components capable of running optimization routines and orchestrating the RAN. They receive data from various sources, including Key Performance Measurements (KPMs) and external context information, aggregating this data to gain a centralized view of the network [19].

Using AI and ML algorithms, the RICs determine and apply control policies and actions on the RAN, enabling automatic optimization of network and RAN slicing, load balancing, handovers, and scheduling policies [6].

5) SECURITY

The openness of O-RAN architecture provides operators with increased visibility into network processes and operations, allowing for better control over the network. Operators can monitor and manage the network more effectively, leading to improved security posture. In [18], they detailed how the virtualized nature of O-RAN platforms enables rapid deployment of security patches and updates, support for automated testing and deployment of security measures, streamlines security processes, ensuring consistent and reliable implementation of security controls across the network. Operators can respond swiftly to emerging threats and vulnerabilities, reducing the window of exposure to potential attack. In O-RAN networks, the virtualized Central Units (CUs) are typically deployed in centralized data centers, making it easier to physically secure RAN cryptographic keys. Centralized key management enhances the protection of sensitive information and strengthens the overall security of the network. The O-RAN Alliance has established a dedicated working group to define threat models and security

measures for O-RAN networks, moving towards a zero-trust security model. Zero-Trust Model ensures that all network components are continuously verified and authenticated, mitigating the risk of unauthorized access and insider threats. While Open-RAN offers several advantages, it also raises security concerns. The open and disaggregated nature of the architecture requires robust security measures to protect against vulnerabilities and threats [18].

6) COST REDUCTION AND EFFICIENCY

O-RAN promises potential cost reductions by introducing competition among vendors, reducing capital and operational expenditures, offering virtualisation and cloudification [20] of network functions thereby making network upgrades and application of releases more efficient [21].

B. OPEN-RAN ARCHITECTURE

The O-RAN architecture introduces key features such as the functional split of Central Unit (CU), Distributed Unit (DU), and Radio Units (RU), standardized interfaces, and the RAN intelligent controller (RIC) [22], [23]. The central unit (CU) serves as the network's central controller, managing multiple DUs and RUs. The O-RAN architecture establishes a hierarchical network management system with both central and distributed controllers. Additionally, the RIC employs AI techniques to embed intelligence across all layers of the O-RAN architecture, enhancing overall network efficiency and performance. O-RAN architecture in Figure 3 covers the scope of O-RAN security, including the O-RAN interfaces (A1, O1, O2, E1 and Open Fronthaul), and the O-RAN components (Service Management and Orchestration (SMO), Non-Real Time RIC, Near-Real Time RIC, O-CU-CP, O-CU-UP, O-DU, O-RU, O-Cloud and O-eNB). The O-Cloud constitutes a cloud computing platform that consists of a set of physical infrastructure nodes capable of hosting essential O-RAN functions, accompanying software components, and the necessary management and orchestration functions. One of the primary objectives of Open RAN is to "open up" the interfaces among various RAN components, encompassing radios, hardware, and software. The O-RAN Alliance has delineated new interfaces, which include A1, O1, E1, F1, open fronthaul M-plane, and O2. These interfaces interwork with 3GPP interfaces. A1 facilitates the connection between the non-real-time RAN Intelligent Controller (RIC) within the SMO framework and the near real-time RIC for RAN optimization. O1 supports all Open RAN network functions when linked with SMO, and O2 establishes a connection between SMO and O-Cloud, enabling the provision of cloud computing resources and workflow management. The open fronthaul M-plane interface serves to establish a connection between the Open Distributed Unit (O-DU) and the Open RAN radio unit (O-RU), refer to Figure 2 for a pictorial view of 3GPP vs O-RAN interfaces. In this section, we discussed these open interfaces and their functions.

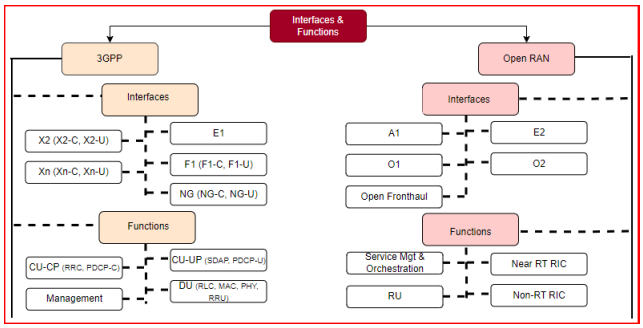


FIGURE 2. 3GPP vs. O-RAN interfaces and functions.

1) RADIO UNIT (RU)

The RU is responsible for transmitting and receiving radio signals to and from mobile devices. It is typically located at cell sites or on cell towers, hosting the lower PHY layer, in addition to overseeing the digital beamforming functionality. In the Open-RAN architecture, RUs should support open interfaces, allowing them to be compatible with different DU and CU components.

2) DISTRIBUTED UNIT (DU)

The DU is a network element responsible for processing and forwarding radio signals to the Core Network. It handles baseband processing and provides a centralized point for controlling and managing multiple RUs (higher PHY layer). Open interfaces, such as the O-RAN fronthaul interface, connect the DU to the RU. Open-RAN relies on standardized, open interfaces that enable interoperability between different components from various vendors. Depending on the functional split option, the DU can support a subset of 4g and 5G radio functions.

3) CENTRALIZED UNIT (CU)

The CU is another network element in the Open-RAN architecture responsible for central processing, orchestration, and network management. It may control multiple DUs and RUs. The CU facilitates centralized management and coordination of network resources. The open interfaces include: O-RAN interfaces, which define specifications for interoperability between RUs and DUs, and X2 interface which enables communication between DUs in a multi-vendor environment. The Orchestration software can automate tasks and adapt the network to changing conditions. CU splits into CU-CP and CU-UP, Control Plane and User Plane respectively. The CU carries out the elevated functionalities associated with Radio Resource Control (RRC) and Packet Data Convergence Protocol (PDCP) within the RAN.

4) NON-RT RIC

The Non-RT RIC (Non-Real-Time RAN Intelligent Controller) operates in non-real-time or non-time-sensitive operations within the network, unlike the Near-RT RIC (near-real-time), facilitating RAN closed-loop control with

timescales larger than 1 sec [24], [25] and supports the rApps implementation from third-parties. Non-RT RIC provides policy management, configuration management resource management, analytics and Reporting: It collects and analyzes network data to provide insights for long-term network optimization and planning. The Non-RT RIC operates with a longer decision-making timeframe compared to the Near-RT RIC. It is focused on tasks that do not require immediate responses to dynamic network changes. It collaborates with various network components, such as base stations, radio units, and the Near-RT RIC, to gather data and exchange information. This interaction enables it to make informed decisions and manage network resources efficiently, optimise and provide data-driven decision making, thereby contributing to the overall network performance by implementing policies, AI/ML models, RAN analytics, model training to aid the functioning of Near-Real-Time RIC [26] and configurations that align with the operator's objectives and service quality standards. Relevant examples of rApps for non-RT RAN control applications include frequency and interference management, RAN sharing, performance diagnostics, end-to-end Service Level Agreement (SLA) assurance and network slicing [26]. To enable a versatile architecture that allows the real-time customization of network components and functions to align with operator goals, the non-RT RIC presents two primary management and orchestration services: policy and intent-based network management via the intent interface [27], [28], data enrichment, QoS priotisation [29].

5) NEAR-RT RIC

The Near-RT RIC (Near-Real-Time RAN Intelligent Controller) operates in near-real-time to address dynamic network conditions. It performs time-sensitive functions such as resource orchestration, load balancing, dynamic spectrum management, and interference management. Operating with minimal latency, it interacts with network elements including base stations and radio units, making rapid decisions to adapt the network to dynamic conditions [30]. The Near-RT RIC ensures efficient resource utilization, maintains high network performance, and dynamically optimizes the RAN to meet the quality of service (QoS) requirements of services and users by establishing connections with the O-CU-CP, O-CU-UP, and O-DU through the standardized open E2 interface. Additionally, it communicates with the Non-RT RIC and the Service Management and Orchestration (SMO) framework via the A1 and O1 interfaces [31].

A1 is the interface connecting the Non-RT RIC and Near-RT RIC, facilitating policy-driven directives for Near-RT RIC applications and accommodating AI/ML workflows. Hoffmann and Kryszkiewicz [32] proposed the use of xApps to detect signalling storm at the beginning of device registration procedure in their paper signaling storm detection in IIoT Network based on the Open RAN Architecture. Their proposed solution using the O-RAN architecture helps

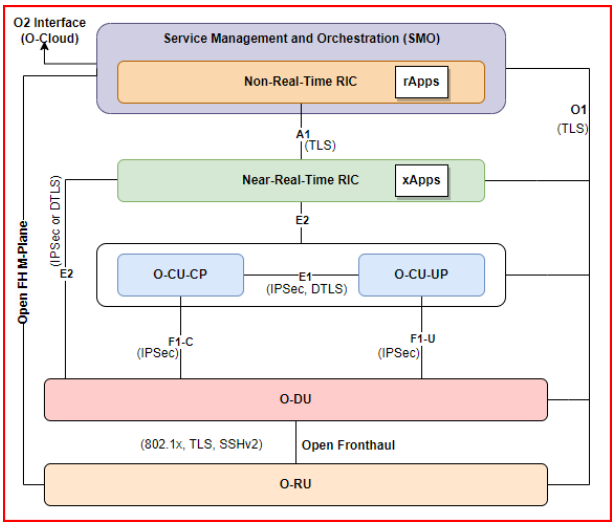


FIGURE 3. O-RAN architecture with interface security mechanisms.

detect Signaling Storm Attacks (SSA) by utilizing O-RAN interfaces to capture network messages and statistics to detect the abnormal activity of adversaries. The xApp proposed in the paper intercepts control plane messages to learn the required long-term network statistics, which are then used to detect the abnormal activity of adversaries at the beginning of their registration procedure.

Lastly, the interaction between Non-RT RIC and Near-RT RIC can be employed for optimizing and refining intelligent AI/ML algorithms, including those associated with load balancing, mobility management, multi-connection control, QoS management, and network energy conservation [33].

6) SERVICE MANAGEMENT AND ORCHESTRATION

Service Management and Orchestration (SMO) facilitates the efficient control and coordination of network services. This component is responsible for a range of vital functions such as service creation, modification, and termination, fault, configuration, accounting, performance, and security (FCAPS), ensuring network services adhere to established policies and standards. It also involves service orchestration, which automates the coordination of various network functions, enabling the creation of seamless end-to-end service chains. O-RAN Service Management and Orchestration leverages policy-driven management to define rules and guidelines for service handling, as well as integrates artificial intelligence (AI) and machine learning (ML) technologies for predictive maintenance and network optimization. The resource allocation, network monitoring, and automation capabilities of this component further enhance O-RAN network efficiency and adaptability. The security requirements in O-RAN WG11 establish a comprehensive security and control framework for the SMO component, focusing on authentication, authorization, resilience against DDoS attacks, secure communications, external interface security,

event logging, and support for OAuth 2.0. These measures aim to safeguard the integrity, confidentiality, and availability of SMO functions and their interactions within the telecommunications network.

C. STANDARDIZATION

Open-RAN is dependent on open standards, a characteristic that presents both advantages and challenges. Firstly, this reliance on open standards allows for enhanced interoperability among various network components, fostering a more flexible and vendor-diverse ecosystem. This promotes innovation and competition within the telecommunications industry. Secondly, open standards support the development of a more accessible and cost-effective network infrastructure. However, on the flip side, the open nature of these standards can potentially become a double-edged sword. While they promote interoperability, they can also introduce threats if not adhered to diligently. Inconsistent or lax adherence to open standards might expose the network to vulnerabilities and security threats, requiring meticulous monitoring and adherence to best practices to mitigate potential risks. In summary, Open-RAN's utilization of open standards offers opportunities for flexibility, innovation, and cost-effectiveness, yet it necessitates a vigilant commitment to security and standards compliance to prevent vulnerabilities and ensure network resilience. There are standards bodies that furnish guidelines and standards for organizations, and operators, encompassing the design, deployment, operations, and overall security guidelines of the Open-RAN systems.

1) ORAN WORKING GROUP 11 (FORMERLY THE SECURITY FOCUS GROUP)

This entity has expedited the development of security specifications, ensuring comprehensive coverage of all security requirements. The WG11 (Working Group 11) is tasked with establishing the necessary criteria and outlining the architectures and protocols for ensuring security and privacy within O-RAN systems. This involves gathering security requirements and proposed solutions from various other working groups (WGs), harmonizing these to ensure consistency across relevant WGs, and ultimately establishing a standardized security framework. The WG11 is responsible for defining security requirements, architectures, and frameworks [23] that align with the open interfaces defined by other O-RAN WGs, thus encompassing security guidelines across the entire O-RAN architecture. The key areas of focus for WG11 include specifying O-RAN security architecture and protocols [22], developing security requirements, defining security protocol profiles and test cases, managing a Coordinated Vulnerability Disclosure (CVD) Program, establishing security guidelines and requirements for the O-RAN Open-Source Community (OSC), contributing to the O-RAN Open Test and Integration Center (OTIC) by integrating and validating security use cases and capabilities, conducting security analysis including threat and risk assessments, and exploring the potential adoption of blockchain technologies within O-RAN security architecture, if deemed feasible [25], [34], [35], [36], [37].

2) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST has crafted cybersecurity guidelines and standards specifically tailored for O-RAN systems, including the Cybersecurity Framework and the Security and Privacy Controls for Information Systems and Organizations.

3) FEDERAL COMMUNICATIONS COMMISSION (FCC)

The FCC has issued guidelines pertaining to wireless network security, encompassing O-RAN systems. These guidelines address aspects such as access control, encryption, and intrusion detection.

4) EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

ENISA has formulated guidelines for the security of 5G networks, incorporating O-RAN systems. These guidelines span areas like threat intelligence, security monitoring, and incident response.

5) NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

NTIA has released a report on the security of O-RAN systems, offering recommendations for enhancing network security.

6) INTERNATIONAL TELECOMMUNICATION UNION (ITU)

The ITU has established security standards for 5G networks, including O-RAN systems, covering aspects like network security architecture, threat analysis, and security management.

7) UNITED STATES DEPARTMENT OF DEFENSE (DOD)

The DoD has outlined security requirements for O-RAN systems, which encompass the utilization of encryption, access control, and intrusion detection.

Standards Development Organizations (SDOs), such as 3GPP SA3 and ETSI security groups, have provided foundational security specifications for 5G networks. They are collaboratively working to develop and implement additional cross-SDO security specifications.

The O-RAN architecture, distinguished by its openness and distributed characteristics, but has introduced new potential areas of threat in contrast to the conventional RAN architecture. Open RAN aims to transform traditional, proprietary, and closed RAN into open, inter-operable, and software-driven systems [6]. This has fueled some research interests in the security of Open RAN using various intrusion systems and algorithms, use of Artificial Intelligence (AI) and Machine Learning (ML) to produce effective solutions within Open RAN security [4], [5], [7], [19], [38], [39]. Attanayaka et al., examined the application

of Federated Learning (FL) to detect anomalies within the O-RAN architecture, emphasizing its ability to safeguard data privacy. They presented a Peer-to-Peer (P2P) FL (Federated Learning)-driven anomaly detection approach tailored for the O-RAN architecture and conduct a thorough analysis of four different variations of P2P FL techniques. This technique on anomaly detection mechanism for O-RAN architecture works by training FL models locally at Near-RT RICs (RAN Intelligent Controllers) and communicating only the parameters for aggregation, thus preserving data privacy and improving communication efficiency. The local trainers of the FL model are hosted at Near-RT RICs, which may reside in the edge clouds, whereas the P2P communication may occur via inter-edge cloud connections. The training model and the detector can be deployed as dedicated xApps, or they can be parts of the same xApp. The advantages of using this mechanism are further described. Firstly, it eliminates the single point of failure, and the parameters are not required to be transmitted to a centralized cloud, thus enhancing the overall security of the network. Secondly, it is more resilient to a single point of failure, making it suitable for hierarchical networks such as O-RAN. Thirdly, it is more efficient in terms of communication and computation, as it trains models locally and communicates only the parameters for aggregation, thus reducing the communication overhead and preserving data privacy. Fourthly, it is more suitable for detecting anomalies in a complex O-RAN environment due to the hierarchical closed-loop architecture of RICs and data-driven inputs via open interfaces. In next section, we will discuss key security threats in O-RAN, present insights on some mitigation strategies and evolution of security in RAN.

TABLE 2. Evolution of security in RAN.

Era	Key Security Developments
Early Cellular Networks (1G and 2G)	• In the early days of telco networks, security was rudimentary. The primary focus was on voice communication, and networks were relatively closed and proprietary. • Basic authentication, encryption was minimal, and data privacy was not of primary concern.
3G and UMTS	• Enhanced encryption and authentication mechanism • Introduction of SIM cards for subscriber identity and verification. • Privacy and data protection became more prominent with the use of encryption algorithms like Kasumi for voice and data security
4G/LTE	• The transition to 4G/LTE marked a significant shift in RAN security. The networks became more IP-based, offering higher data rates and a broader range of services • Security features such as mutual authentication between the network and devices, robust encryption (AES) • Introduction of firewalls and Intrusion Detection Systems (IDS) were implemented • Home Subscriber Server (HSS) for better user authentication and authorization were introduced
5G	• 5G Security architecture introduced network slicing with end-to-end security. • Enhanced security protocols such as 5G-AKA for strong authentication and encryption. • NFV and SDN in 5G networks introduced new Security challenges.
O-RAN and Diverse Ecosystem	• Security for open interfaces. • Protection against security threats and privacy becomes the sine qua non • Mutual authentication and integrity protection. • O-RAN ALLIANCE standards for Open RAN.
Future Challenges	• IoT, edge computing, and URLLC unique security requirement. • IDS, AI/ML will play important role threat detection and mitigation in O-RAN. • Quantum-safe cryptography exploration required to protect RAN networks against future threats from quantum computing.

III. SECURITY REQUIREMENTS, CHALLENGES, AND PROPOSED SECURITY TAXONOMY IN OPEN RAN

In this section, we look at the threats in Open RAN and develop a threat taxonomy in Open RAN. Furthermore, we provide a detail description of the two main categories of Open RAN threat. The evolution of security in RAN has been marked by significant advancements to address the growing complexity of mobile networks and the ever-evolving threat landscape. Here, we provide a detailed overview of the key stages in the evolution of RAN security. These are driven by the need to protect networks and users from an ever-expanding range of threats. As technology advances, RAN security will adapt to ensure the confidentiality, integrity, and availability of services in an increasingly connected and dynamic world.

A. OVERVIEW OF SECURITY CHALLENGES IN OPEN RAN

Undoubtedly, incorporating novel architectural elements, open interfaces (as illustrated in Fig. 2), multi-vendor nature, network disaggregation, and the integration of tailored and potentially data-driven control logic will enhance the efficiency and flexibility of next-generation cellular networks. However, this transformative shift with relevant nascent technologies [40], the incorporation of extra interfaces and nodes, coupled with the separation of hardware and software, broadens the network's vulnerability and exposure to potential threats and attacks, thereby introducing a set of unique security risks and challenges [41]. These challenges primarily arise from the distributed and disaggregated nature of the O-RAN infrastructure, which significantly expands the potential attack surface for malicious actors, thus posing significant threats to the network. Simultaneously, the advanced monitoring capabilities, intelligence, and cloud-native deployment features inherent to O-RAN architectures provide valuable insights into network status

and furnish the essential tools for implementing advanced solutions for monitoring, detecting, preventing, and mitigating threats, but could support in launching attacks. To address these concerns, the O-RAN Alliance has established a dedicated working group responsible for analyzing and defining threat models for O-RAN networks [34]. This group is also tasked with formulating security measures and policies for the various components within the O-RAN architecture [23], [42] In summary, while Open RAN offers many benefits, including flexibility and vendor diversity, these threats, including supply chain security risks, and virtualization vulnerabilities plus threats posed by the integration of AI/ML need urgent attention [14]. Some of the unique security risks and challenges associated with O-RAN will be discussed in this section.

B. THE SECURITY REQUIREMENT FROM O-RAN ALLIANCE

O-RAN WG11 provided security threat modelling and risk assessment [34] detailing various potential vulnerabilities in O-RAN components, emphasizing the risks associated with insecure designs, outdated components, and insufficient update management. These vulnerabilities could lead to unauthorized access through different interfaces, enabling attackers to inject malware, manipulate software, harm components, create performance issues, or reconfigure systems. The ultimate goals for attackers may include eavesdropping, wiretapping, denial-of-service attacks, and stealing sensitive data. WG11 raised specific concerns about misconfigurations in O-RAN components, with potential exploits including weak authentication and access control. Attacks on O-RAN networks may exploit design flaws, improper configurations, and weak security measures on web servers. The increasing prevalence of IoT devices in the context of 5G O-RAN introduces the risk of Distributed Denial of Service (DDoS) attacks. Open interfaces in O-RAN, such as Fronthaul, O1, O2, A1, and E2, are identified as potential points of vulnerability if they lack proper security measures. Issues such as improper authentication, authorization processes, and insecure implementations of TLS or SSH protocols could make O-RAN components susceptible to attacks. Furthermore, security breaches due to insufficient authentication and authorization mechanisms pose a significant risk, allowing attackers to compromise O-RAN components and perform various malicious activities. Additionally, concerns are raised about the compromise of monitoring mechanisms, integrity of log files, and adherence to industry best practices for securing sensitive data handled by O-RAN components. They looked at the security requirements for SMO to encompass providing authentication support for both SMO functions and External Systems, enabling authorization for internal and external requests (i.e., ensuring confidentiality, integrity, mutual authentication, and replay protection), and ensuring resilience against volumetric DDoS attacks across various interfaces and internal communications, with the capability for efficient logging and security controls [23]. In terms of security controls, the requirements include supporting an OAuth 2.0 authorization server with a token endpoint, OAuth 2.0 resource owner/server, and client functionalities for service requests. Additionally, enabling mutual authentication of SMO functions using mTLS with PKI X.509v3 certificates and potential authentication with TLS using a pre-shared key (PSK). For rApps, security requirements involve supporting authorization capabilities for Non-RT RIC as a resource owner/server and client, enabling recovery from volumetric DDoS attacks across various interfaces, and implementing authentication for both API Producers and Consumers across the R1 interface using a Kafka-based protocol. Security controls for Non-RT RIC include supporting OAuth 2.0 resource owner/server for A1-EI, OAuth 2.0 client for A1-P, and potentially TLS and OAuth 2.0 authorization for the R1 interface, as specified in O-RAN Security Protocols Specifications. The security requirements and controls for xApps in the Near-RT RIC include authenticating xApp access to the Near-RT RIC database, providing authorized access, mutual authentication in communication between xApps and Near-RT RIC platform APIs, an authorization framework for xApp service consumption, support for authorization as a resource owner/server and client, recovery from DDoS attacks, and defense against content-related attacks. Additional security controls include mutual TLS authentication for transactional APIs, Internet Protocol Security (IPsec) for time-critical APIs, OAuth 2.0 authorization for transactional APIs, and verification of policies received through the A1 interface. For the Y1 interface, security controls include mutual TLS authentication, OAuth 2.0 authorization, and TLS support for data confidentiality, integrity, and replay protection.

C. OPEN RAN SECURITY TAXONOMY

We present two key categories of Open RAN Security as depicted in Figure 4 as technical and non-technical threats.

1) TECHNICAL THREATS

In the landscape of Open RAN, where the traditional boundaries of network architecture are being redefined, technical threats (Infrastructure, application, network interception, interface and protocol vulnerability, and access control threats) pose significant challenges. These threats target the core technological components that form the backbone of Open RAN systems, encompassing a range of potential vulnerabilities that could impact the security, reliability, and overall performance of the network. Addressing these technical threats is crucial for ensuring the robustness of Open RAN deployments and maintaining the integrity of next-generation telecommunications infrastructures.

a: INFRASTRUCTURE ATTACKS

In this section we look at the threats in Open RAN security that are associated with the use of cloud, hypervisor, virtualization and orchestration technologies. These are integral to the disaggregated architecture of Open RAN. Hypervisor

vulnerabilities represent a significant concern, as exploits in the hypervisor could lead to unauthorized access and control over the entire virtualization infrastructure. The potential for VM isolation and escape poses a security risk, where vulnerabilities or human error and misconfigurations [43] might allow an attacker to move from one virtual machine to another, compromising sensitive network functions. Also, [44], they looked at the insecure APIs and misconfigured management interfaces within Open RAN components and how they can be exploited by attackers to manipulate or disrupt the operation of virtualized network functions. Resource exhaustion attacks targeting CPU, memory, or storage in virtualized environments can degrade the performance of network functions or lead to denial-of-service conditions. Ensuring secure communication between virtual machines is vital, as vulnerabilities in inter-VM communication could expose sensitive information to eavesdropping or interception [45]. The complexity of virtualized environments requires robust visibility and monitoring tools to detect and respond to security incidents effectively. Regular patch management is essential to address known vulnerabilities, as failure to update the virtualization infrastructure may expose the network to exploitation of security flaws. Compliance with industry standards and regulations is crucial for virtualization in Open RAN, and failure to meet these standards may lead to legal and regulatory consequences.

b: APPLICATION ATTACKS

There are five major categories identified under application attack: data and model poisoning attacks, firmware API attack, logging attack and Evasion attacks. Soltani et al. [46] introduced a novel attack called Bearer Migration Poisoning (BMP) in the Open-RAN architecture of 5G networks. BMP aims to mislead the Radio Intelligent Controller (RIC) into triggering a malicious bearer migration procedure. The adversary manipulates the RIC's perception to believe that a bearer context migration procedure needs to be initiated. By doing so, the adversary can release a valid bearer context between Distributed Unit (DU) and Centralized Unit-User Plane (CU-UP) and establish a new bearer context towards the target CU-UP. This manipulation of the bearer context can lead to significant network anomalies such as routing blackholes, impacting the overall performance of the O-RAN network. Additionally, the BMP attack results in a dramatic increase in signalling costs, network latency [47], and wastage of radio resources, ultimately affecting the user experience and service quality in the network. Two prominent issues were identified - a) signalling costs (approximately ten times higher than the normal scenario), and b) drop in throughput (causing catastrophic drops in throughput, with downlink and uplink throughput decreasing to nearly 0 Mbps). The increase in signalling cost is attributed to the malicious manipulation of bearer migration procedures, which results in a higher signalling overhead in the network. To help detect the malicious manipulation of bearer migration procedures and prevent the attack from being successful, the authors proposed to leverage packet inspection techniques to gain insight into the exchanged messages between the RIC, CU-CP, and xApp. Another possible solution is to redesign the bearer context migration procedure or patch the RIC to address the vulnerability that allows the BMP attack to occur. This approach can provide a comprehensive defense against the attack and ensure the integrity and reliability of the O-RAN network

c: THREATS FROM INTEGRATING WITH AI/ML

AI/ML offers advantages such as energy savings in Open RAN, network optimization, and device management, however, it brings along security threats, as adversaries can manipulate imported AI/ML data and models to corrupt or influence outcomes. Despite the potential for Open RAN to enhance detection and response with AI/ML, caution is necessary to address the associated security concerns. Also, adversarial attacks can manipulate data during training or serving, potentially misleading AI-based slice admission models and causing them to wrongly reject RAN slice requests [48]. To address these security threats, [49] proposes the implementation of a moving target defense (MTD) strategy. This strategy aims to prevent poisoning attacks by adding uncertainty to the system, making it harder for attackers to predict and exploit vulnerabilities. Specifically, the proposed MTD strategy involves dynamically picking a model from a set of PPO models trained with different configurations, thereby increasing the adversary's uncertainty and enhancing the robustness of the solution against adversarial attacks. This proactive resilience approach aligns with the MTD paradigm, which continually changes the attack surface to make it more challenging for attackers to exploit vulnerabilities. By incorporating the MTD strategy, [49], [50], [51], [52], [53], [54], [55] aims to bolster the security of the O-RAN architecture, particularly in the context of AI/ML-based dynamic service admission control and power minimization, thus mitigating the impact of potential adversarial attacks. The proposed approach utilizes mathematical methods and the proximal policy optimization (PPO) algorithm to address the problem on two-time scales within the O-RAN architecture.

Firstly, on a large time scale, the approach employs mathematical methods to determine the optimal number of predefined Virtual Network Functions (VNFs) for each slice. This involves solving mathematical models based on the mean arrival delay and the mean service time of the system at different times of network traffic. Secondly, on a smaller time scale, the approach leverages the proximal policy optimization (PPO) algorithm, which is an actor-critic deep reinforcement learning (DRL) technique. This is used to dynamically solve the problem of service admission control and power minimization for different slices within the O-RAN architecture. The PPO algorithm enables the system to adapt and optimize its decision-making processes in

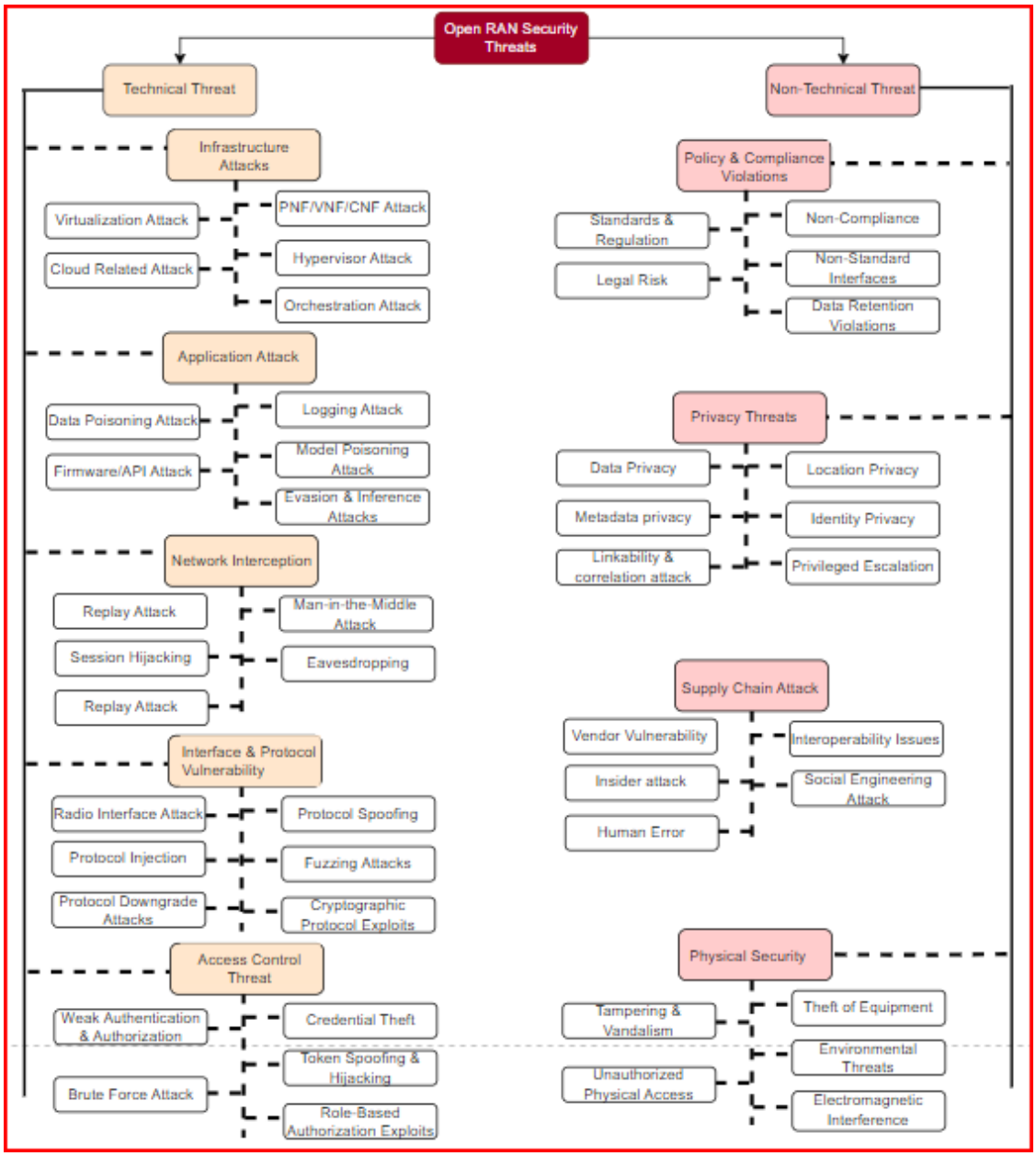


FIGURE 4. Open RAN security taxonomy.

real-time based on feedback and environmental changes. The results show that the proposed PPO-based service admission control approach achieves an admission rate above 80 percent indicating its capability to effectively manage and control service admission within the O-RAN architecture. Additionally, the experimental outcomes highlight the effectiveness of the moving target defense (MTD) strategy in strengthening the robustness of the PPO method against adversarial attacks, as evidenced by the significant improvement in the system's performance in adversarial scenarios.

In [49] Motalleb et al., implemented a Moving Target Defense (MTD), a proactive security strategy that involves continuously changing the attack surface of a system, making it more challenging for attackers to predict and exploit vulnerabilities. This approach aims to enhance the resilience of a system against evolving threats by adding ambiguity and complexity, thereby reducing the effectiveness of potential attacks. In the context of the O-RAN architecture and AI/ML-based systems, MTD can be implemented by dynamically altering system configurations, such as shuffling AI models or network components, to increase uncertainty and make it more difficult for adversaries to launch successful attacks. By continually changing the system's attack surface, MTD aims to lower the success rates of attacks and improve the overall security posture of the system.

d: NETWORK INTERCEPTION

Five prominent attacks are identified under network interception namely - Man-in-the-Middle attack, replay, session hijacking, eavesdropping attacks [56]. Man-in-the-Middle (MitM) attacks on the communication interface between network controllers in the O-RAN architecture can have significant consequences as highlighted in [57]. In their test case on consequences of MitM attack, Tiberti et al., executed Ettercap (on A1 interface) on an attacker-controlled virtual machine, connected to O-RAN controllers in the same sub-network. Ettercap employs ARP Cache Poisoning through Gratuitous Reply messages to manipulate the victim's ARP Table, redirecting its communications to the attacker. When TLS is used for secure communication, the attacker may bypass it through techniques like SSL Strip, where they impersonate the recipient during the TLS handshake, or acting as a proxy server by injecting their certificate into the sender's certificate store, allowing them to manipulate or intercept traffic. Attackers who gain access to the controller's internal network can exploit the lack of strong authentication mechanisms to retrieve, manipulate, and forward network policies. This can lead to potential data leakage, denial of service, and traffic flow manipulation. The attack can result in the arbitrary overwriting of existing policies, causing inconsistency in the stored policies between the two network controllers. These consequences underscore the critical importance of securing the communication interface to prevent such attacks and their potential impact on the network. In [12], they looked at vulnerabilities at each plane and explained how an intruder has the capability to falsely present itself as an O-DU and introduce its own control messages into the O-RU. These injected messages may be crafted to achieve a specific behavior in U-plane packets or could be deceptive, leading to a Denial-of-Service (DoS) situation in the O-RU. By injecting misleading data into authentic control messages exchanged between the O-DU and O-RU, the attacker can once again degrade the O-RU's performance. Furthermore, the attacker may identify, intercept, store, delay, or repeatedly re-transmit a specific uncorrupted control message, causing disruptions. These types of attacks can also be initiated from the O-RU to the O-DU, affecting the northbound components of the network. Therefore, securing the C-Plane necessitates the implementation of the following security features: Authenticity, ensuring only legitimate O-DUs and O-RUs communicate with each other; Integrity, confirming that messages remain unaltered during transmission; Confidentiality, guaranteeing the privacy of every message; and Replay Protection, ensuring messages are received at the intended moment. In the U-Plane, similar to the C-Plane, it faces security threats such as impersonation, DoS attacks through packet injection, and passive wiretapping. An attacker may manipulate or redirect user data messages using a rogue base station. To address these concerns, security measures like Authenticity, Integrity, Confidentiality, and Replay Protection are essential for securing the U-Plane. The fronthaul link requires strict performance assurance due to precise synchronization between O-DU and O-RU. Attacks on synchronization, such as impersonating clocks or injecting false packets, can compromise network operation. In the S-Plane, delay and packet removal attacks have a more significant impact, causing inaccurate PTP offset calculations and synchronization mismatches. To secure the S-Plane, features like Authenticity, Integrity, Confidentiality, and Replay and Delay Protection are essential. The M-Plane, operating in the application layer and secured by TLS or SSH, poses a direct threat only if security is compromised. However, Layer-2 threats affecting other planes can impact the M-Plane, leading to potential denial of service (DoS) incidents. To secure the M-Plane, measures such as Authenticity, Integrity, Confidentiality, and Replay Protection are necessary. Considering the four pillars of security (Confidentiality, Integrity, Authenticity, and Availability), it is evident that the O-FH faces various threats, posing a high risk to the overall performance of the O-RAN and its users. Despite O-RAN's adoption of open and well-known protocols and tools (TLS 1.3 with mutual authentication, a carefully chosen set of cipher suites, stringent access control rules for interfaces and resources, and the incorporation of support for intrusion detection systems and SIEM stacks (e.g., ELK)), it is imperative to address vulnerabilities arising from the architecture and its alignment with various implementation scenarios.

A replay attack transpires when an assailant intercepts and maliciously retransmits previously recorded data with the intent to deceive one or more network elements. The attacker intercepts legitimate communications, storing them for subsequent replay to gain unauthorized access or manipulate the network's behavior. The attack can target signaling messages, control plane data, or even user data transmissions within the Open RAN by exploiting the openness and flexibility of the architecture. Replay and eavesdropping attacks in Open RAN often focus on communication channels, including fronthaul, midhaul and backhaul interfaces, rendering them susceptible to interception. Attackers can eavesdrop on communication between baseband units (BBUs), remote radio units (RRUs), and other network elements, capturing critical information for later replay. By replaying legitimate commands or signaling messages, attackers can manipulate the behavior of network elements, potentially resulting in unauthorized access, service disruption, or injection of malicious commands into the Open RAN, compromising overall network security. Effectively mitigating replay attacks in Open RAN necessitates a blend of cryptographic techniques, secure communication protocols, and intrusion detection mechanisms. Utilizing mechanisms such as timestamping, sequence numbers, and cryptographic nonces aids in detecting and rejecting replayed messages. Implementation of secure key exchange protocols further fortifies the resistance of the Open RAN architecture to replay and eavesdropping attacks. Continued research into enhancing encryption algorithms, secure key management, and intrusion detection mechanisms is imperative to bolster

the resilience of Open RAN against evolving replay and eavesdropping attack vectors.

Lastly, Session hijacking in Open RAN security involve the unauthorized interception and manipulation of active communication sessions in O-RAN architecture and subsequently assumes control of the session. This form of attack is characterized by the jamming and interception of session-related data, enabling the attacker to manipulate the ongoing communication, in most cases by exploiting the weaknesses in authentication and authorization mechanisms within Open RAN. Attackers may compromise user credentials or exploit vulnerabilities in the authentication process, allowing them to impersonate legitimate users or network elements and gain access to active sessions. Effectively mitigating session hijacking in Open RAN necessitates a comprehensive approach such as strengthening authentication mechanisms, implementing secure session management practices, and incorporating encryption for session data are pivotal steps. Continuous monitoring for abnormal session behavior and the implementation of intrusion detection systems enhance the network's capability to promptly detect and respond to session hijacking attempts. Given the dynamic nature of Open RAN deployments, the development of adaptive security measures becomes crucial for staying ahead of emerging threats associated with session hijacking. This adaptability is essential to address evolving attack vectors and maintain the robust security posture of Open RAN networks. The architecture of O-RAN enables direct access to physical layer (PHY) measurements through interfaces linked to RAN Intelligent Controllers (RICs) and the potential execution of specialized analysis via dedicated xApps or rApps. This openness in interfaces, coupled with the capability to analyze wireless traffic metrics and exchange control messages within RIC using dedicated xApps or rApps, renders the O-RAN architecture highly adept at detecting jamming attacks [58]. Their study introduces a statistical approach for detecting downlink jamming, leveraging link quality reports from User Equipments (UEs), and discusses its integration into O-RAN. The paper delves into the threat of jamming attacks in 5G networks, proposing a statistical method utilizing link quality reports from UEs for downlink jamming detection. Furthermore, it explores the implementation of this method within the framework of O-RAN architecture, presenting performance metrics derived from simulations. The authors underscore O-RAN's suitability for jamming attack detection owing to its interface openness and capacity for wireless traffic analysis and control message exchange in RIC via dedicated xApps or rApps. Ultimately, the paper concludes that the proposed method effectively detects downlink jamming in 5G networks and can be seamlessly integrated into O-RAN architecture, exhibiting promising performance metrics.

e: NETWORK AND PROTOCOL VULNERABILITY

The researchers in [10], [21], and [59], delved into vulnerabilities within the radio interface of Open RAN. These studies identify potential threats such as unauthorized access and service disruption [60], emphasizing the need for robust encryption and continuous updates to radio protocols to mitigate these risks. Cao et al. [61] discussed the broader spectrum of network vulnerabilities, highlighting threats to network integrity. Their study underscores the importance of intrusion detection systems and anomaly detection mechanisms to address unauthorized control and service disruption within Open RAN networks. The work of [62] focuses on network vulnerabilities, specifically addressing redirect attacks. The research emphasizes the necessity of secure authentication mechanisms and stringent validation checks to counter unauthorized access resulting from deceptive communication in Open RAN protocols. In their analysis, [63] shed light on Protocol Injection vulnerabilities, emphasizing the exploitation of communication protocols, while offering some mitigation strategies to include the importance of regular updates, patching protocols, and deploying intrusion detection systems to thwart unauthorized control and system vulnerability exploitation. The research by [64] delves into cryptographic aspects of Open RAN security. It emphasizes the significance of using robust cryptographic algorithms (quantum-resistant) and ensuring regular updates to cryptographic protocols to counteract threats such as cryptographic protocol injection and maintain confidentiality and integrity. Further, to mitigate protocol downgrade attacks, [65], [66] propose the implementation of secure negotiation mechanisms, vigilantly monitoring protocol negotiation attempts to prevent the compromise of encrypted communication and the overall security. In conclusion, the development of adaptive security frameworks and real-time threat intelligence integration or IDS will enhance the resilience of Open RAN networks against evolving network and protocol vulnerabilities.

f: ACCESS CONTROL THREAT

To understand the impacts of access control threats in Open RAN, first we provide some basic details on authentication and authorisation types such as Knowledge-based Authentication, Possession-based Authentication, Multi-Factor Authentication, and Risk-based Authentication. Knowledge-based Authentication method relies on information known only to the legitimate user. A password, for instance, is an exemplar of ''something you know.'' Presuming the user keeps the password confidential to prevent credential theft or brute force attacks, it can serve as a means of authentication. Secret questions also fall within this realm. In Possession-based Authentication, authentication technique depends on the possession of an object essential for verification, held exclusively by the genuine user. Assuming the user securely maintains the artifact, its possession can validate the user's identity. Examples of possession-based authentication include key fobs generating codes, codes sent to mobile devices, and physical keys. Identity-based Authentication method relies on unique, non-falsifiable user

attributes. In contemporary systems, this typically involves biometric readings such as fingerprints, iris scans, voice prints, etc., compared against a baseline reference. Multi-Factor Authentication combines muliple authentication forms, such as knowledge-based and possession-based. Multi-Factor Authentication solutions integrate three or more authentication methods. Risk-based Authentication describes an adaptive authentication approach that adjusts identity verification challenges based on a) the user's adherence to a usage profile established and maintained by the application. This encompasses information used to identify the user, such as typical usage patterns, common operations, IP addresses used, geolocation, browser fingerprints, etc. b) attempts to access highly sensitive features or information. In Open RAN, the effectiveness of an authentication mechanism directly corresponds to its resistance against unauthorized access. Naturally, the strength of authentication within a system should align with the significance of the assets it safeguards. Hence, employing two-factor and multi-factor, certificate-based authentication solutions is pertinent within the Open RAN architecture. Weak Authentication in Open RAN denotes situations where the authentication method lacks adequate robustness relative to the importance of the assets under protection. It also encompasses instances where the authentication and authorisation mechanism exhibits flaws or susceptibility to breaches. To address weak authentication and authorization threats, Open RAN deployments implement strong, multi-factor authentication methods, regularly update access control policies, and conduct thorough security audits. Additionally, the adoption of zero-trust security models can enhance overall network resilience [52]. Robust authentication and authorization practices with RBAC contribute to a more secure Open RAN environment, mitigating the risks associated with unauthorized access and manipulation.

2) NON-TECHNICAL THREATS

Beyond the intricacies of technology, Open RAN implementations face a spectrum of non-technical threats (policy and compliance violation, privacy, supply chain and physical security) that stem from various external factors. These threats extend beyond the realms of code and hardware, impacting the operational, regulatory, and even geopolitical aspects of Open RAN ecosystems. Navigating through these non-technical challenges is essential for establishing a secure and resilient Open RAN environment, as the success of this paradigm shift relies not only on technological advancements but also on adept management of diverse non-technical risks.

a: PHYSICAL SECURITY

Physical security of Open RAN infrastructure is of paramount importance, as vulnerabilities in this domain can compromise the integrity, availability, and confidentiality of the network. We explore the various physical threats encountered in Open RAN deployments and the measures taken to mitigate them. Unauthorized access to the management interface of an unprotected O-RU poses a significant threat, potentially allowing attackers to illicitly obtain private keys, certificates, hash values, inject malware, or manipulate existing O-RU software. This vulnerability could lead to various malicious activities, including launching denial-of-service, intrusion, and replay attacks on other network elements, such as an O-DU. To mitigate these risks, hardening the O-RU platform becomes crucial, substantially reducing the potential attack surface. Security measures for the O-RU span three key aspects: supply chain security, which ensures a secure chain of custody from manufacturing to installation; physical security, involving tamper-resistant seals and secured ports; and network security, encompassing authentication, communication security protocols, TPM procedures for software upgrades, and various hardening features like disabling unnecessary components and interfaces, secure boot, and hardware-based security modules.

b: VANDALISM, THEFT AND ENVIRONMENTAL HAZARDS

Open RAN components, such as radio units (O-RUs) and antennas, are often deployed in outdoor environments, making them vulnerable to vandalism and theft. Malicious actors may tamper with or steal these components, leading to service disruptions or unauthorized access to sensitive data. Therefore, adequate physical security measures, including tamper-resistant design and surveillance, are necessary to mitigate these risks. Also, Open RAN infrastructure is exposed to various environmental hazards, including extreme weather conditions, natural disasters, and wildlife interference. These hazards can damage equipment, disrupt network connectivity, and compromise service availability. Deploying ruggedized enclosures, weatherproofing materials, and redundancy in critical components can help mitigate the impact of environmental threats.

c: ELECTROMAGNETIC INTERFERENCE (EMI)

The RUs are susceptible to electromagnetic interference from nearby sources such as power lines, radio transmitters, and electronic devices. EMI can degrade signal quality, increase error rates, and disrupt network operations. Proper grounding, shielding, and electromagnetic compatibility (EMC) testing are essential to minimize the effects of EMI on Open RAN infrastructure.

d: UNAUTHORIZED ACCESS

Physical access to Open RAN components can be exploited by unauthorized individuals to gain privileged information, tamper with equipment, or launch cyber-physical attacks. Fo the deployment on the cloud (private or public cloud), adequate measures shall be put in place to physically secure the infrastructure and the data centre sites. For example, Amazon Web Services (AWS) adopts a shared responsibility model, where AWS is responsible for the security of the cloud, whereas the customers are responsible for the security in the cloud [67], [68]. However, for RUs, securing access

to Open RAN sites through access controls, authentication mechanisms, and monitoring systems can help prevent unauthorized access and safeguard critical infrastructure.

e: SUPPLY CHAIN THREATS

Open RAN ecosystems are characterized by a diverse array of stakeholders, including hardware and software vendors, integrators, service providers, and open-source communities. This diversity amplifies the complexity of the supply chain, as each participant introduces their own set of security risks [69], [70]. This openness and disaggregation inherent in Open RAN introduce a myriad of supply chain threats that must be effectively managed to ensure the security and integrity of deployments. Drawing insights from recent literature, we present a detailed examination of supply chain threats in Open RAN and propose strategies for mitigating these challenges.

f: INCREASED ATTACK SURFACE

Compared to traditional proprietary architectures, Open RAN architectures expose a larger attack surface due to the expanded number of parties involved in the supply, development, maintenance, and operation of the technology. This increased attack surface heightens the risk of supply chain attacks [71], including malicious hardware or software insertion, tampering, or unauthorized modifications.

g: ESPIONAGE AND IMBALANCE CONCERNS

The inclusion of high-security risk companies within the Open RAN Alliance raises concerns about espionage possibilities and disruptions to the intended openness of the ecosystem. Dominance by partners from one country or region could lead to imbalances in the development and standardization process, compromising the integrity and security of Open RAN.

h: MITIGATING STRATEGY

Promoting diverse participation in Open RAN development efforts can mitigate the risk of dominance by a single entity or group, enhancing openness, transparency, and accountability. Enhance security measures within the supply chain by rigorously vetting partners, implementing secure communication channels, and adopting encryption technologies to mitigate the risk of espionage and disruptions. As a future-proof proposal, blockchain technology offers a potential solution for securing infrastructure and enhancing transparency within Open RAN ecosystems. Its decentralized and immutable nature can mitigate the risk of fraud, manipulation, and supply chain disruptions by providing a transparent ledger of transactions. [72] argued that the integration of firmware authentication codes, a permissioned blockchain ledger, and equipment node validators ensures the security of open RAN equipment by embedding unique identifiers and hashes into firmware, utilizing a blockchain ledger for transparent tracking across the supply chain, and validating firmware authenticity during deployment, the system establishes a tamper-resistant ecosystem, enhancing supply chain security and preventing compromised devices from entering the network.

In the blockchain sector, Federated Learning (FL) presents a robust framework for safeguarding data sharing, enabling various entities to securely exchange information while upholding confidentiality. Within the realm of blockchain technology, integrating O-RAN and FL holds promise for bolstering data privacy and security within decentralized networks. This integration ensures that user data stays within the jurisdiction of individual participants, thereby diminishing the risks of data breaches and unauthorized entry [73].

IV. INTRUSION DETECTION SYSTEMS FOR OPEN RAN

Intrusion detection is a method responsible for recognizing anomalous data (outliers) that deviate from the typical data patterns (inliers). These anomalous data are termed anomalies and are categorized into distinct types. For example, Outliers manifest as brief or minor abnormal patterns, like communication errors; change in events denotes sudden notable shifts, such as extreme weather conditions, while drifts are marked by slow, unidirectional, and long-term changes in data, such as sensor faults. Intrusion detection can be implemented as a software or hardware component that continuously monitors the network, detecting and alerting authorised users to any malicious activities it detects [74]. The primary objective of an IDS is to recognize unauthorized or malicious behavior occurring within the network or systems, promptly reporting such incidents to enhance the security and protection of the network or systems against potential threats [75].

In the O-RAN context, intrusion detection algorithms pinpoint abnormal behavior in network data, such as signal power or communication among nodes. Various approaches can be employed for anomaly detection, including machine learning algorithms [4] based on (1) decision trees, classification, or statistical models, (2) clustering like K-means, where anomalies do not fall within a cluster, and (3) deep reinforcement learning, specifically designed to handle high-dimensional data and multiple features. Other ML classifications include naive bayes, support vector machines (SVM), clustering (K-Means and Hierarchical), logistic regression, and random forest [38].

An intruder within an O-RAN ecosystem may fall into one of the following categories:

- **Internal Intruder:** These are factors or groups with authorized access and privileges within the organization who aim to misuse resources and exploit assets. Internal attacks (these are related to non-technical threats discussed in Section III) could involve manipulating critical data, disclosing confidential information, or engaging in data theft
- **External Intruder:** These are factors from outside the network who lack the rights or privileges to access

the network. Attackers employ various techniques or policies to destroy the normal functioning of the system

A. TYPES OF INTRUSION DETECTION SYSTEMS

- **Signature-Based IDS:** These intrusion detection systems, also known as Misuse Detection, utilize pattern-matching techniques to identify attacks by comparing potential intrusions against previously recorded incidents in a database [76]. While effective at recognizing known attacks, they may fail to detect zero-day (unknown/new) attacks due to the absence of signatures. However, Signature-Based IDSs offer the benefit of increased processing speed for known attacks and help in minimizing false alarms.
- **Anomaly-Based or Network-based IDS (NIDS):** Unlike Signature-Based IDSs, anomaly-based intrusion detection systems excel at detecting and alerting on unknown suspicious behaviors. Instead of relying on a signature database to identify threats, anomaly-based IDSs utilize machine learning to train and model the detection system. Initially, these systems model regular network and system behaviors, and any deviations from this modeled normal behavior are flagged and reported as potential attacks.
- **Heuristic-based IDS (HIDS):** relies on predefined rules or heuristics to identify potentially malicious activities. These rules are crafted based on the characteristics and behaviors typically associated with known attacks. Instead of relying on specific signatures, heuristic-based IDSs analyze patterns of behavior to detect anomalies that may indicate an intrusion.
- **Hybrid Method:** refers to approaches that combine multiple detection techniques or methodologies. These methods may integrate signature-based detection, anomaly-based detection, heuristic analysis, machine learning algorithms, or other approaches to enhance intrusion detection's overall effectiveness and accuracy.
- **Machine Learning-Based IDS:** leverages algorithms and statistical models to analyze network or system data and detect abnormal patterns or behaviors that could indicate malicious activity. These systems learn from labeled training data to identify and adapt to new threats, making them particularly effective for detecting previously unseen attacks or zero-day vulnerabilities.
- **Behavior-Based IDS:** focuses on monitoring and analyzing the behavior of users, applications, and devices within a network to detect deviations from normal behavior. Instead of relying solely on signatures or known patterns of attacks, behavior-based IDSs establish baselines of normal behavior and trigger alerts when activities deviate significantly from these baselines. This approach effectively detects insider threats, zero-day attacks, and other sophisticated attacks that may evade traditional detection methods.

TABLE 3. Intrusion detection types.

IDS	HIDS	NIDS	WIDS	NBA
Components	Management and database server	Sensor (in-line/passive), Management and database server	Sensor (passive), Management and database server	Sensor (mostly passive), Management and database server
Detection scope	host	Network and Scope	WLAN client	Network and host
Network architecture	Managed network or standard network	Managed network	Managed network or standard network	Managed network

Next we provide a comparison of the core components of Intrusion Detection Systems in traditional RAN and Open RAN in Table 4.

B. IDS IN O-RAN AND SPECIFIC SECURITY CONCERNS

To discuss the exploration of security concerns specific to Open-RAN, including virtualization threats, interconnection vulnerabilities, and the role of third-party vendors it is essential to understand the distinct environment of O-RAN networks which are described in the next section.

The identification of the new advancements and challenges for IDS in Open-RAN networks for real-time monitoring and rapid response are detailed in Section VI.

C. IDS DEPLOYMENT STRATEGY IN OPEN-RAN

Deploying IDS in Open-RAN networks requires a multi-layered approach, with sensors placed at various points in the network to monitor both user plane and control plane traffic. Leveraging virtualization and automation technologies enables flexible and scalable deployment of IDS to protect against a wide range of security threats. Briefly, we present a review of the placement of IDS sensors and the flow of network traffic. This is followed by comparative analysis of IDS architectures: Centralized, Distributed, Edge, and Cloud-Based IDS.

1) PLACEMENT OF IDS SENSORS

- **Radio Unit (RU):** IDS sensors can be deployed at the edge, directly on the RU, to monitor traffic at the radio interface. This enables detection of radio-specific attacks and anomalies, such as radio jamming or rogue base stations.
- **Distributed Unit (DU):** IDS sensors can also be placed at the DU, which serves as an aggregation point for multiple RUs. Monitoring traffic at this point allows detection of attacks targeting the fronthaul network connecting RUs to DUs.
- **Centralized Unit (CU):** IDS sensors can be deployed at the CU, which handles higher-level functions such as baseband processing and network management. Monitoring traffic at this level helps detect attacks

TABLE 4. Comparison of IDS Components: Traditional RAN vs. Open-RAN.

	Traditional RAN	Open-RAN
DATA SOURCES	• Network Traffic: This includes packet-level data, logs from network devices (e.g., routers, switches), and flow data. • System Logs: generated by network elements, servers, and other devices within the RAN provide valuable insights into system activities, user authentication, and access attempts. • Event Logs: from security appliances, such as firewalls, intrusion prevention systems (IPS), and authentication servers, help identify security events and potential threats. • Sensor Data: from physical or virtual sensors deployed throughout the RAN infrastructure can provide additional context for detecting security anomalies.	• Network Traffic: Data from O-RAN fronthaul, midhaul interfaces, virtualized infrastructure. • System Logs: Logs from virtualized infrastructure, cloud resources.and containerized applications, provide insights into system activities, resource utilization, and potential security incidents. • Event Logs: from security appliances, authentication servers, and other network elements remain relevant in O-RAN environments. IDS in O-RAN should integrate with these devices and services to capture security-related events and correlate them with other data sources for enhanced threat detection. • Sensor Data: Sensor data from physical or virtual sensors (including network performance metrics) deployed throughout the O-RAN infrastructure continues to provide additional context for detecting security anomalies.
ANALYSIS ENGINE	• Signature-Based Analysis: Compare against known attack signatures. • Anomaly-Based Analysis: analyze and detect deviations from normal behavior • Heuristic Analysis: Apply predefined rules for suspicious activities, crafted based on the characteristics of known attack methods and vulnerabilities.	• Signature-Based Analysis: Inspect traffic across diverse platforms. • Anomaly-Based Analysis: Detect deviations in dynamic O-RAN environment where dynamic scaling, resource sharing, and varying traffic patterns are common. • Heuristic Analysis: Identify risks associated with third-party components (customization, and integration), emerging threats or vulnerabilities.
RESPONSE MECHANISM	• Alerting: When the IDS detects a potential security threat or anomaly, it generates notification alerts on detected event, severity level, and recommended actions. • Automated Actions: In some cases, IDSs may be configured to automatically respond to detected threats or anomalies. This can include blocking malicious traffic, quarantining compromised devices, or initiating incident response procedures. • Logging and Reporting: IDSs typically maintain logs of detected events and responses for forensic analysis and compliance purposes.	• Alerting: Alerts should include detailed information about the nature of the incident, virtual machine affected with possibility of lateral effect, its severity level, and recommended mitigation actions. • Automated Actions: In O-RAN, where automation and orchestration play a significant role, IDS may leverage automation frameworks to orchestrate responses to detected security incidents. Automated actions may include traffic redirection, policy enforcement, isolation of compromised components, or triggering incident response workflows. • Logging and Reporting: comprehensive logs of security events, responses, and remediation actions for auditing, compliance, and forensic analysis purposes. Reporting to provide insights into security posture, incident trends, and emerging threats within the O-RAN ecosystem.

targeting the control plane and management interfaces of the network.

2) FLOW OF NETWORK TRAFFIC

- **User Plane Traffic:** In Open-RAN, user plane traffic flows between the RU and the DU, carrying data between the mobile devices and the core network. IDS sensors deployed at the RU or DU can monitor this traffic for anomalies such as malware propagation or DDoS attacks.
- **Control Plane Traffic:** Control plane traffic involves signaling and management messages exchanged between network elements for configuration and control purposes. IDS sensors deployed at the CU can monitor this traffic for signs of protocol anomalies or unauthorized access attempts.
- **Management Traffic:** Management traffic includes communication between network management systems and the RAN components for configuration, monitoring, and maintenance. IDS sensors deployed at the CU can monitor this traffic to detect unauthorized access or malicious commands.

3) VIRTUALIZED COMPONENTS

O-Cloud comprises a collection of computing assets and virtualization infrastructure consolidated within one or multiple physical data centers [77]. This framework integrates physical nodes, software elements (such as operating systems, virtual machine hypervisors, etc.), and management and orchestration features [78], [79]. In virtualized deployments of Open-RAN, IDS sensors can be instantiated as virtual network functions (VNFs) running on the same hardware platform as other network functions. This allows for flexible scaling and resource allocation based on traffic load and security requirements.

4) ORCHESTRATION AND AUTOMATION

Orchestrating the deployment of IDS sensors in Open-RAN networks can be done through network automation platforms that manage the lifecycle of virtualized network functions. This includes provisioning, scaling, and updating IDS instances as needed to adapt to changes in network topology or traffic patterns.

5) IDS ARCHITECTURES

- **Centralized IDS:** The Centralized Intrusion Detection System employs a centralized approach by strategically deploying specialized monitors across the network. These monitors are assigned the task of observing network traffic and host behavior. Subsequently, the data collected from monitoring activities is directed to a central analysis unit. CCIDS serves a dual

purpose: data collection and threat detection. Monitors diligently gather data, while the central analysis unit aggregates information from various sources. Moreover, the analysis, correlation, and subsequent threat detection processes are centralized. CCIDS is characterized by centralized management and configuration, facilitating efficient control over intrusion detection operations. This architecture is particularly effective in hierarchical network structures or environments with centralized control mechanisms. Nonetheless, CCIDS may encounter scalability challenges due to its dependence on a central analysis unit, warranting careful consideration in extensive network deployments.

- **Distributed IDS:** The system employs a distributed architecture, with monitors strategically positioned throughout the network, functioning independently as analysis units interconnected through a peer-to-peer framework. These monitors autonomously process, aggregate, and analyze data within their designated network segments, collaborating in real-time to enhance threat detection and response. Workload distribution across monitors ensures resource efficiency and optimized system performance. Key characteristics of the architecture include scalability advantages, resilience to failures, and flexibility for individual monitors to adapt to diverse network environments independently. Overall, the distributed approach facilitates efficient threat detection and response while maintaining system resilience and flexibility in dynamic network environments.
- **Edge IDS:** This represent a pivotal advancement in network security architecture, addressing threats at the network's perimeter or "edge." With the expanding reach of edge computing and the Internet of Things (IoT), traditional network boundaries have shifted, necessitating robust security measures at the edge. Edge IDS solutions cater to this demand by deploying intrusion detection capabilities closer to data generation points, thereby augmenting threat visibility, responsiveness, and resilience. On top of its ease of integration feature for most detection techniques such as signature-based, anomaly detection and machine learning algorithms, edge IDS can integrate threat intelligence feeds to enhance detection accuracy and responsiveness, enabling proactive defense against emerging threats. Notably, edge IDS offer advantages such as reduced latency, bandwidth optimization, enhanced privacy and compliance, and resilience to network outages. Analyzing network traffic at the edge enables minimal latency in threat detection, crucial for real-time applications. Additionally, by processing sensitive information locally, edge IDS enhance data privacy and compliance with regulatory requirements, such as GDPR or HIPAA.
- **Cloud-Based IDS:** Cloud-Based Intrusion Detection Systems (IDS) are integral components of modern cybersecurity frameworks, offering scalable and adaptive security solutions tailored to the dynamic nature of cloud environments. By leveraging the scalability, elasticity, and computational power of cloud platforms, cloud-based IDS deploy virtual sensors within cloud environments to monitor network traffic, system logs, and application behavior in real-time. These sensors collect vast amounts of data, providing comprehensive visibility into cloud infrastructure and services. A centralized analysis engine hosted on the cloud platform correlates and analyzes data collected from virtual sensors using advanced detection techniques, such as signature-based detection, anomaly detection, and machine learning algorithms. Integration with cloud service provider APIs enables seamless monitoring and analysis of cloud resources, while the incorporation of threat intelligence feeds enhances detection capabilities. Cloud-based IDS offer advantages such as scalability, cost-efficiency, global visibility, rapid deployment, and automatic updates and maintenance. However, challenges including data privacy and compliance, network latency, and security controls must be carefully considered. Use cases for cloud-based IDS include cloud infrastructure protection, compliance monitoring, threat hunting, incident response, and multi-cloud security. As cloud adoption continues to accelerate, the importance of cloud-based IDS in safeguarding sensitive data, maintaining compliance, and protecting against evolving cyber threats will become increasingly pronounced, urging organizations to embrace cloud-based IDS as an integral component of their cybersecurity strategy in Open RAN.

D. SECURITY SOLUTIONS AND THEIR BENEFITS IN OPEN RAN

O-RAN is dedicated to advancing radio access networks, prioritizing intelligence and openness as its core principles. The goal is to propel the mobile industry toward an ecosystem characterized by innovation, multiple vendors, interoperability, and autonomous RAN. This approach aims to reduce costs, enhance performance, and increase agility [80]. The O-RAN Alliance adheres to key principles, including leading the industry towards open, interoperable interfaces, RAN virtualization, and integrating big data and AI for RAN intelligence. It also emphasizes using common-off-the-shelf hardware and merchant silicon while minimizing proprietary hardware. Furthermore, the Alliance specifies APIs and interfaces, promotes standards adoption, and explores open-source solutions where appropriate [24].

1) INNOVATIVENESS

By transitioning from a closed vendor environment to a standardized, multi-vendor, AI-powered hierarchical controller structure, O-RAN allows RAN vendors, operators, and third parties to deploy innovative services as RAN applications. This shift bring some benefits and enables

the leveraging of emerging technologies to deploy a more advanced security solutions, such as AI-based security, blockchain-based security, and quantum-safe security [2]. Madhusanka et al., outlined the benefits of Open RAN, to include full visibility, selection of best modules, diversity, and modularity. Through open interfaces, operators can gain full visibility into network performance and operational telemetry data. This visibility, isolated from executing environments, facilitates early detection of security issues and root cause analysis. However, it also poses challenges in identifying accountability across vendors, potentially complicating security review processes. Practices such as 'secure by design' DevSecOps and collaboration with vendors in Continuous Integration/Continuous Deployment (CI/CD) processes enhance security and influence vendor offerings. In this context, patch management and operational agility, capability to deploy upgrades independently and explore innovative security measures, enabling swift vulnerability remediation and transparent updates becomes a common practice within Open RAN environment.

2) DIVERSITY

Open RAN empowers network operators to enhance security protocols and swiftly address threats by integrating technologies and methodologies from diverse industries. Drawing insights from advancements in these fields, telecom operators can leverage extensive expertise in safeguarding intricate systems. With Open RAN's accessible interfaces, operators can adopt a holistic security strategy, enhancing oversight and governance across the network. This facilitates comprehensive data analysis, enabling operators to detect potential vulnerabilities and promptly mitigate security breaches [81].

3) COST

The fact that Open RAN can contribute to lower total cost of ownership (TCO) with reduced expenditure on infrastructure and maintenance [82], [83], would mean that operators have more resources available to allocate towards security enhancements [84]. In fact, in [85], Open RAN is projected to become 30% more cost-effective than existing proprietary options due to the integration of open-source technologies and contributions from various software vendors within an open ecosystem. This increased budget allows for the implementation of advanced security measures and the adoption of cutting-edge technologies to fortify network defenses. By prioritizing security within Open RAN deployments, operators can effectively mitigate risks while maximizing their investment, ultimately enhancing the reliability, confidentiality, and integrity of cellular communication services.

In conclusion, the fusion of Open-RAN and edge computing represents a monumental transformation in RAN network. This convergence ushers in the dynamics of distributed systems and edge device security, imparting layers of complexity to security management. Network operators navigating this transformative landscape must remain vigilant, adopting a multifaceted security strategy such as anomaly-based IDS that encompasses access controls, encryption, monitoring, and auditing. The security of Open-RAN and edge computing is a multifaceted puzzle that, when assembled with diligence and precision, ensures the integrity, confidentiality, and resilience of modern networks in an era where data is of paramount importance.

TABLE 5. Comparison of Suricata, Snort, and Zeek (formerly Bro).

Feature	Suricata	Snort	Zeek (formerly Bro)
Description	High-performance Network IDS, IPS, and NSM	Open-source Network IDS and IPS	Network analysis framework for traffic analysis
Protocol Support	Wide range including IPv4, IPv6, TCP, UDP, HTTP, TLS/SSL, and more	Wide range including IPv4, IPv6, TCP, UDP, HTTP, SMTP, and more	Comprehensive support for various protocols including DNS,HTTP, SSH, SSL, IRC, SMTP,
Performance	Multi-threaded engine for high performance	Single-threaded, but efficient	Efficient protocol analysis and metadata extraction
Detection Mechanism	Signature-based detection, anomaly detection	Signature-based detection	Signature and anomaly-based IDS
Rule Language	YAML-based configuration, Suricata rules, ETOpen rules	Snort rules	Bro script language
File Extraction	Supported	Limited support	Not typically used for file extraction
TLS/SSL Decryption	Supported	Supported	Not typically used for TLS/SSL decryption
Customization	Flexible configuration options	Customizable rule language (Snort rules)	Highly customizable with Bro script language

Next, in Table 5, we present a quick overview on the features of some open-source IDS tools that can be applied in Open-RAN, such as Suricata, Snort, and Zeek.

V. CASE STUDIES

In this section we present real-world case studies where IDS was implemented in Open-RAN networks with outcomes, challenges, and lessons learned from these implementations.

Cost reduction, flexibility, ecosystem expansion, and support for new service models are the key drivers for the adoption of Open RAN, but there are potential risks perceived by operators such as the nascence of technology, standards, and the supply chain. The immaturity of the current open RAN specifications, ecosystem, and Open RAN security are seen as the barriers to deployment. More activity is expected in new deployments like enterprise or private 5G RANs, where operators do not have to integrate legacy equipment. These are referred to as secondary networks, and

a diverse range of service providers, including MNOs, private network operators, neutral hosts, cable operators, cloud providers, and enterprises, are likely to be involved [86]. Secondary networks are seen as more suitable for testing new architectures than primary macro networks due to their lower coverage and traffic demands, greenfield status, and reduced criticality to the core business. Open RAN is expected to make faster progress in such scenarios. The O-RAN Alliance has a dedicated Security Working Group that focuses on addressing security challenges in Open RAN deployments. While they provide guidelines and specifications rather than specific implementations, their efforts contribute to establishing best practices for Open RAN security. In this section, we focus on some real-world case studies on Open RAN deployments from early adopters (Rakuten Mobile (Japan), Vodafone (Various Regions), Telecom Infra Project (TIP) and Telefonica) and how they have integrated security in Open RAN.

In the realm of IT, the separation of hardware and software occurred quite some time ago. This separation gave rise to specialized software entities operating in distinct horizontal layers. The software developed by these entities became versatile, capable of running on various hardware platforms, thereby offering operators and customers a diverse range of choices. Simultaneously, a thriving ecosystem of hardware providers also emerged. In the telco space, Open RAN brings extra interfaces that are 'open', calling for the need for innovativeness and increased horizontal players. These open interfaces outlined in the Open RAN technical specifications offer heightened independent visibility and the potential for an overall improved and more secure system. The Open RAN network functions align with broader cloud network functions, sharing similar security requirements and solutions. Cloud architecture ensures resilience, scalability, and segmentation, incorporating advanced features like AI/ML and Multi-Access Edge Computing (MEC) [87]. Utilizing MEC, for instance, enables the localization of DDoS detection, intrusion detection and mitigation at the network's edge, isolating incidents from the rest of the network. Enhanced security measures such as micro-segmentation, containerization, virtualization, and network slicing are integral to the system design, providing robust protection from the hardware level up [88]. This approach contrasts with traditional systems, where security measures are typically added on after the system is established. By leveraging 3GPP's 5G NR architecture, Open RAN also inherits advanced security features introduced for 5G, encompassing enhanced user identity privacy (Subscription Concealed Identifier - SUCI), comprehensive protection of control/user plane traffic between the UE and gNB (via encryption and integrity protection) over the air interface, safeguarding gNB interfaces such as E1 between CU-CP and CU-UP, and F1 between CU and DU, improved home network control through authentication, and supplementary security provisions for network slices based on Service Level Agreements (SLA).

Rakuten Mobile, in their paper "A Definitive Guide to Open RAN Security," underscores the significance of security in their Open RAN architecture [89]. Their approach includes principles such as mutual authentication, access control, and secure runtime environments. They emphasize the importance of unified identity, credential, and access management based on zero-trust network access principles, secure API protection, and a policy-driven architecture for dynamic system configuration. Rakuten Mobile outlines a comprehensive set of security principles, covering mutual authentication, access control, the principle of least privilege, secure runtime environments, domain separation, measures against lateral movement, data protection, secure bootstrapping, and best practices for open source components. These principles collectively aim to fortify the security of Rakuten Symphony's Open RAN architecture, and they provides detailed insights into their implementation and influence on security architecture for Open RAN in their deployment.

A. OPEN RAN SECURITY FRAMEWORK IMPLEMENTATION

The primary objective of the O-RAN ALLIANCE is to establish a secure, open, and interoperable RAN. Drawing inspiration from standards development organizations like 3GPP and The Internet Engineering Task Force (IETF), the O-RAN ALLIANCE WG11 mission is to devise an O-RAN security architecture that empowers 5G service providers to implement and manage O-RAN with the same confidence as a 3GPP-defined RAN.

The WG11 leads and collaborates with other O-RAN ALLIANCE working groups to ensure that O-RAN is inherently secure. O-RAN's openness and disaggregated architecture offer inherent security advantages, including transparency and common control through open-source software, interoperability of secure protocols and features via open interfaces, and supply chain security through disaggregation. However, the expansion of the O-RAN architecture with new interfaces and functions introduces new security risks, with heightened complexity, making in-house deployment a formidable challenge particularly when considering virtual and cloud-based deployments [90]. Open-source software, whitebox hardware, and the multi-party relationships involved in these deployments contribute to shared security risks. Providers are urged to adopt a risk-based approach in Open RAN deployments. Recognizing these challenges, the WG11 follows 3GPP security design practices and industry best practices to define security requirements and solutions. The WG11 is actively engaged in creating a series of documents to enhance O-RAN architecture security. Notable documents include the Security Threat Modeling and Remediation Analysis, which offers a thorough examination of threats to O-RAN assets; the Risk Assessment document [34], providing an impact assessment based on ISO 27005 [91] and considering internal and external attacks; and Security Protocol Specifications [22] and Security Requirements Specifications [23], outlining

high-level requirements for the use and configuration of security protocols such TLS1.2, TLS1.3, DTLS 1.2, SSHv2, IPSec, OAuth 2.0, control policies such RBAC (Role-Based Access Control) and cryptographic operations for integrity, authenticity and confidentiality on Open RAN interface deployments. Furthermore, the WG11 is developing a security guidelines document for vendors participating in the O-RAN Software Community (OSC). The group is also exploring the application of cutting-edge technologies such as blockchain for mutual authentication and distributed identity management, zero-touch provisioning, and artificial intelligence to bolster O-RAN security. In conclusion, the O-RAN architecture adopts a Security-by-Design approach by bringing security-related aspects into consideration from the design phase. This means that security is not an afterthought, but rather a fundamental aspect of the architecture, platform, and data (data at rest, data in transit) [12].

B. ZERO-TRUST NETWORK DEPLOYMENT

Open RAN security embraces the Zero Trust architecture, centered on the principle of ''distrust, until verified''. It ensures protection through network segmentation, thwarting lateral movement, Layer 7 threat prevention, and precise user-access control. WG11 is actively working on a Zero Trust Architecture (ZTA) for Open RAN by conducting analyses of both external and internal threats. The goal is to define security requirements and controls for Open RAN's attack surface, aiming to mitigate potential threats. This effort involves incorporating guidance from NIST [92], ESF [93], and EU NIS [94]. The National Cybersecurity Strategy of the United States Office of the National Cyber Director (ONCD) advocates the implementation of a Zero Trust Architecture (ZTA) within the critical infrastructure of 5G [95], and the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) has formulated Security Guidance for 5G Cloud Infrastructure [93]. These guidance urges operators and suppliers to adopt zero trust architecture in their deployments. The Zero Trust architecture, rooted in cybersecurity principles, aims to prevent data breaches and limit internal lateral movement by extending protection to all enterprise assets. In this approach, enterprises assume no implicit trust, consistently analyzing risks, and implementing protective measures, including restricting access to resources and ensuring continual authentication and authorization [96]. To uphold a Zero Trust architecture, each O-RAN component are deployed with specific functionalities and protections outlined by the O-RAN Alliance, encompassing integration with external identity management, role-based access control, encryption, integrity protection and security log generation. Rakuten Symphony presents a Zero Trust Network (ZTN)-based solution for Identity and Access Management (IAM). This solution encompasses identity management, role and permission administration, single sign-on, robust authentication methods, and dynamic policy-driven access control for various network infrastructures, including cloud-native platforms. The security posture in Open RAN deployment assures mobile network operators (MNOs) that their Open RAN deployments are secure, whether implemented on-premises or in a private, public, or hybrid cloud environment, instilling confidence in the overall deployment process.

The IAM solution plays a crucial role in provisioning identities and credentials for users, machines, and applications. This facilitates the establishment of secure communications among users and devices, users and applications, and between different applications. Objects such as devices, hosts, containers, services, and applications constitute various resources that subjects seek to access. The access control decisions are made by a generic authorization gateway or proxy, taking into account the subject's identity, device identity, and contextual factors like the requester's location, access time, connection method to resources, and device security posture. The management of access permissions is simplified through a role-based access control model.

C. SECURE API TRANSACTIONS

Rakuten's deployment incorporates an API gateway that serves as a centralized service that receives incoming API requests from clients, directs these requests to the appropriate application service, processes the service's response, and relays the response back to the requesting client. This external gateway for managing API requests enhances application security and simplifies communication management. Role-based access control (RBAC) addresses permissible user behavior, aligning with the zero-trust concept of ''''distrust, until verified''. This approach ensures enforceable least privilege access to services within the mesh, upholding the principle of least privilege in a cloud-native platform.

D. SECURE DEVOPS IMPLEMENTATION

In implementing Secure DevOps (DevSecOps) for Open RAN, operators are taking an approach to embed security measures seamlessly into the development, deployment, and operational phases. Their strategy encompasses the integration of security tools, ensuring the integrity of Infrastructure as Code (IaC), and safeguarding containerized components. Continuous security testing is prioritized, employing automated scans for vulnerabilities, penetration testing, and security assessments at early stages of the development and throughout the software development lifecycle. Test phase management is crucial for protecting sensitive information, and cross-functional collaboration and training sessions promote a security-aware culture across development, operations, and security teams. Continuous monitoring tools are deployed for real-time detection of security incidents, with an incident response plan integrated into the overall DevOps workflow. Automated compliance checks and a feedback loop for continuous improvement ensure that security processes evolve in response to emerging threats and lessons learned from incidents.

This Secure DevOps implementation in Open RAN is characterized by its holistic approach, combining proactive security measures with automated testing, ongoing collaboration, and a commitment to continuous improvement. By seamlessly integrating security practices into every stage of the development and deployment lifecycle, operators maintain the speed and efficiency of DevOps while bolstering the security posture of their Open RAN infrastructure.

VI. FUTURE DISCUSSIONS

In this section, we discussed a series of new advancements that are gaining momentum in Open RAN security and privacy domains. For example, the application of 5G and Beyond approach to Security, blockchain, AI/ML, and Large Language Model

A. ADAPTING TO 5G AND BEYOND

- **Network Slicing Security:** 5G networks introduce network slicing, allowing multiple virtual networks to coexist on a shared physical infrastructure. Security in Open RAN requires robust isolation between network slices to prevent cross-slice interference and ensure data confidentiality. Techniques such as secure encapsulation, cryptographic isolation, and access control mechanisms are essential to safeguard the integrity and privacy of each network slice.
- **Virtualization Security:** Open RAN leverages virtualized network functions (VNFs) and software-defined networking (SDN) principles to enable flexible and dynamic network configurations. Security measures such as hypervisor security, VNF integrity verification, and secure bootstrapping are necessary to protect against virtualization-based attacks, including hypervisor exploits, VM escape vulnerabilities, and container runtime security risks.
- **Container Security:** Containerization technologies, such as Docker and Kubernetes, are commonly used in Open RAN deployments to package and deploy network functions. Ensuring the security of containers is crucial to prevent container breakout attacks, privilege escalation, and unauthorized access to sensitive resources. Implementing container security best practices, including image signing, runtime monitoring, and access control, helps mitigate container-related security risks in Open RAN environments.
- **Security Orchestration and Automation:** Security orchestration and automation platforms streamline security operations in Open RAN deployments by automating routine tasks, orchestrating incident response workflows, and integrating security controls across heterogeneous environments. Security Information and Event Management (SIEM) systems, Security Orchestration, Automation, and Response (SOAR) platforms, and Threat Intelligence Platforms (TIPs) help organizations detect, investigate, and mitigate security threats more efficiently and effectively.

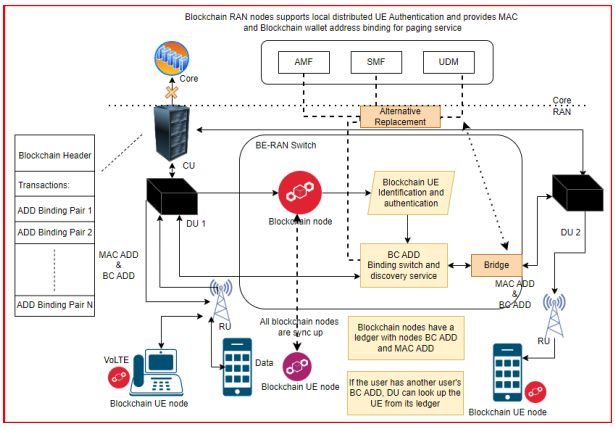


FIGURE 5. Framework for blockchain-enabled RAN.

- **Continuous Monitoring and Threat Detection:** Continuous monitoring and threat detection capabilities are essential for identifying and responding to security incidents in real-time. Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Network Behavior Analysis (NBA) solutions monitor network traffic, detect suspicious activities, and alert security teams to potential threats in Open RAN environments. Leveraging machine learning and artificial intelligence algorithms enhances the accuracy and efficacy of threat detection mechanisms, enabling organizations to proactively defend against emerging cyber threats.

B. INTELLIGENT BLOCKCHAIN INTEGRATION

Blockchain-based security solutions have garnered considerable attention in various domains, including telecommunications, as they offer unique capabilities for enhancing security, trust, transparency, and resilience in network architectures including Open RAN. Below we detail how blockchain can be applied to bolster security in Open RAN.

- **Decentralized Authentication and Immutability:** Blockchain operates as a decentralized and immutable ledger [97], recording transactions across a distributed network of nodes. In the context of Open RAN, [98] utilizes Blockchain's decentralized authentication protocols to enable mutual authentication between entities without the need for a centralized Certificate Authority (CA) as detailed in the Figure 5 [98]. This eliminates the single point of failure and privacy concerns associated with traditional PKI solutions with improved computational efficiency due to reduced communication overhead. Xu et al., framework on Blockchain-Enabled RAN (BE-RAN), includes components such as the BE-RAN switch, Blockchain nodes for UE authentication and privacy-preserving, and VoLTE integration enhancing the communication capabilities of the network. The design features Blockchain-based UE identification and authentication, ensuring secure mutual authentication using private keys and signatures. The MAC frame design incorporates Blockchain addresses for privacy-preserving communication and

efficient data transmission. Also, blockchain can be utilized to maintain a tamper-resistant record of network activities, including resource allocation, authentication events, and configuration changes. This ensures transparency, traceability [99] and integrity, making it difficult for malicious actors to manipulate or tamper with critical network information. Each participant or mode in the Open RAN ecosystem can have a unique digital identity stored on the blockchain [100], which can be cryptographically secured and verified. This mitigates the risk of identity theft, spoofing, and unauthorized access, thereby strengthening overall network security.

- **Decentralized Key Management:** Traditional centralized key management systems pose inherent security risks, as they present single points of failure and potential targets for malicious attacks. By contrast, blockchain enables decentralized key management solutions, where cryptographic keys are distributed across multiple nodes in the network [101]. This distributes the risk of key compromise and enhances resilience against unauthorized access or data breaches. Additionally, blockchain-based key management systems can facilitate secure key exchange and authentication protocols within Open RAN deployments.
- **Supply Chain Integrity:** Supply chain security is a critical concern in Open RAN deployments, as vulnerabilities introduced at any stage of the supply chain can compromise the integrity of the entire network. Blockchain technology can be employed to track and verify the provenance of hardware components, software updates, and configuration changes throughout the supply chain lifecycle [102]. By immutably recording transactional data and cryptographic signatures on the blockchain, stakeholders can ensure the authenticity and integrity of critical assets and mitigate the risk of supply chain attacks.
- **Smart Contracts for Automated Security Policies:** Smart contracts, self-executing contracts with the terms of the agreement directly written into code, can be leveraged to automate security policies and enforcement mechanisms within Open RAN. For example, smart contracts can define access control rules, encryption protocols, and incident response procedures, ensuring consistent and auditable security measures across the network. Additionally, smart contracts can facilitate automated responses to security incidents, reducing response times and minimizing the impact of potential breaches.

C. APPLICATION OF AI/ML IN O-RAN SECURITY

AI/ML based security solutions offer significant potentials for enhancing security in Open RAN deployments.

- **Anomaly Detection:** AI/ML algorithms can analyze vast amounts of network data to establish baseline behavior patterns and detect anomalies indicative of security threats or breaches. By continuously monitoring network traffic, AI/ML models can identify suspicious activities such as rogue RUs/DUs, unusual traffic patterns, or abnormal behavior in network elements. This proactive approach enables early detection and mitigation of security incidents, minimizing the impact on Open RAN operations. Historical security data, threat intelligence feeds, and security incident reports to identify emerging threats and predict potential security risks in Open RAN environments. By leveraging advanced analytics techniques, AI/ML models can forecast the likelihood and severity of future security incidents, enabling proactive measures to mitigate vulnerabilities and strengthen defenses against evolving cyber threats.
- **Behavioral Analytics:** AI/ML algorithms can analyze user and device behavior within the Open RAN network to identify deviations from normal patterns and detect suspicious activities in real-time. By correlating multiple data sources, such as user access logs, device telemetry, and network traffic, AI/ML models providing adaptive security controls can detect insider threats, compromised devices, and unauthorized activities that may pose security risks to Open RAN infrastructure.
- **Threat Hunting and Response:** AI/ML-powered threat hunting platforms can autonomously search for indicators of compromise (IOCs) and potential security threats across the Open RAN environment. By continuously analyzing telemetry data, logs, and network traffic, AI/ML models can identify and prioritize security incidents for investigation and response. Additionally, AI-driven security orchestration and automation tools can streamline incident response workflows, enabling rapid containment and remediation of security threats. Furthermore, AI/ML algorithms can assess the security posture of Open RAN deployments in real-time by analyzing contextual information such as network topology, configuration settings, and vulnerability data. By dynamically evaluating risk factors and threat indicators, AI/ML models can provide actionable insights and recommendations for enhancing security controls, implementing access policies, and allocating resources to mitigate potential security risks.

D. DIGITAL DIVIDE

Digital divide refers to the gap between those who have access to modern information and communication technologies (ICTs) and those who do not. In the context of Open RAN, addressing the digital divide involves ensuring equitable access to wireless connectivity, particularly in undeserved or remote areas where traditional network infrastructure may be lacking. While the digital divide is primarily a socio-economic and accessibility issue, it also has implications for security in Open RAN deployments especially in the non-technical category as explained in Section III. We look at how addressing the digital divide through Open RAN deployments not only improves access

to connectivity but also contributes to security solutions by extending coverage and connectivity, enhancing resilience and redundancy, empowering communities, protecting privacy and data, and ensuring regulatory compliance, thereby contributing to global efforts to achieve universal connectivity and digital inclusion.

- **Extended Coverage and Connectivity:** By deploying Open RAN solutions in undeserved or remote areas, operators can extend network coverage and connectivity to populations that were previously unconnected or undeserved. This helps bridge the digital divide by providing access to essential communication services, such as voice calls, messaging, and internet access, to marginalized communities. From a security perspective, extending network coverage helps reduce the risk of security incidents and vulnerabilities associated with disconnected or isolated environments, such as unauthorized access attempts or unsecured communication channels.
- **Resilience and Redundancy:** Open RAN deployments in undeserved areas can enhance network resilience and redundancy by leveraging distributed architectures and decentralized infrastructure. Redundant network elements, multi-operator support, and interoperable standards ensure continuity of service and reliability, even in challenging environments prone to natural disasters, infrastructure failures, or network outages. This resilience helps mitigate security risks associated with service disruptions, data loss, or downtime, ensuring uninterrupted access to critical communication services for coverage-deprived areas.
- **Community Empowerment and Participation:** Engaging local communities in the deployment and operation of Open RAN networks fosters community empowerment and participation, enabling residents to take ownership of their connectivity infrastructure. Community-driven initiatives, such as community networks or cooperative deployments, empower undeserved populations to address their unique connectivity needs and bridge the digital divide on their own terms. By involving local stakeholders in decision-making processes and capacity-building activities, Open RAN deployments can build trust, foster collaboration, and enhance security through community resilience and vigilance.
- **Regulatory Compliance and Policy Frameworks:** Adhering to regulatory standards and industry best practices ensures that Open RAN deployments meet minimum security requirements and adhere to ethical and legal principles. By promoting transparency, accountability, and compliance with regulatory mandates, Open RAN deployments can enhance trust, legitimacy, and security in undeserved communities, fostering sustainable and inclusive digital development.

E. ADAPTING TO FUTURE LLM TECHNOLOGIES OR SECURE INTENT-DRIVEN TECHNIQUES IN OPEN RAN

Although there are limited research work in this area in Open RAN security, but we have detailed a few areas of interests with promising research work.

- **Enhanced Threat Detection and Intelligence:** Large Language Models (LLMs) powered by advanced natural language processing (NLP) techniques can analyze vast amounts of network data, logs, and communication patterns to identify potential security threats and anomalies. By processing unstructured data sources such as network traffic, system logs, and user behavior, LLMs can uncover hidden patterns, trends, and indicators of compromise (IOCs) that may evade security controls. LLMs can also integrate external threat intelligence feeds, security advisories, and vulnerability databases to enhance threat detection capabilities and provide real-time insights into emerging cyber threats.
- **Intent-driven Security Policies:** Secure Intent-driven techniques enable security policies to be defined based on high-level intents or objectives, rather than specific configurations or rules. By aligning security policies with network requirement, compliance requirements, and user preferences, intent-driven security ensures that security measures are adaptive, context-aware, and responsive to changing network conditions and threats. Intent-driven security policies can enable Open RAN deployments to dynamically adjust security controls based on detected anomalies, policy violations, or predefined security objectives, enhancing the overall resilience and effectiveness of Open RAN security defenses.
- **Automated Response and Orchestration:** Integrating LLM-based threat intelligence with intent-driven security policies enables automated response and orchestration capabilities in Open RAN deployments. LLMs can analyze security events from O-RAN devices, prioritize alerts, and recommend response actions based on predefined security intents and contextual information. Intent-driven security orchestration platforms can automate incident response workflows, trigger response actions, and coordinate remediation efforts across heterogeneous network environments, reducing the time to detect and mitigate security incidents.
- **Continuous Monitoring and Adaptive Controls:** LLM-based security analytics and intent-driven techniques can enable continuous monitoring of network activities, user behavior, and security events in Open RAN deployments. By leveraging real-time telemetry data and predictive analytics, LLMs can detect emerging threats, anticipate security risks, and adapt security controls dynamically to mitigate potential vulnerabilities. Intent-driven security policies can enforce adaptive access controls, encryption protocols, and authentication mechanisms based on contextual factors such as user

location, device type, and network conditions, ensuring consistent protection across diverse Open RAN environments.

- **Collaborative Threat Intelligence Sharing:** LLM-powered threat intelligence platforms can facilitate collaborative threat intelligence sharing and information exchange among Open RAN operators, vendors, and industry stakeholders. By aggregating and analyzing security data from multiple sources, LLMs can identify common attack patterns, threat actors, and attack vectors across different Open RAN deployments. Intent-driven security policies can facilitate secure information sharing, threat attribution, and coordinated response efforts, enabling organizations to collectively defend against cyber threats and enhance the overall security posture of Open RAN ecosystems.

VII. CONCLUSION

In conclusion, IDS in Open RAN networks holds paramount significance in ensuring robust security measures. Throughout this paper, we have emphasized the vital role of IDS in mitigating evolving cyber threats and vulnerabilities inherent in Open RAN architectures. As telecommunications landscapes continue to evolve rapidly, characterized by increasing interface complexity and inter-connectivity, the proactive integration of security measures becomes imperative. IDS serves as a proactive defense mechanism, enabling the identification and mitigation of potential security breaches before they escalate, thereby safeguarding the confidentiality, integrity, and availability of critical network resources. Moreover, in the context of Open RAN, where disaggregated architectures introduce unique challenges, the implementation of IDS becomes even more crucial in fortifying network defenses.

As highlighted in our work, the dynamic nature of cyber threats necessitates a proactive approach to security. Threat modeling, risk assessments, and the adoption of security best practices are indispensable for ensuring the resilience of Open RAN networks in the face of emerging threats. By embracing proactive security measures, stakeholders can effectively mitigate risks and foster the continued innovation and advancement of telecommunications technologies.

In essence, the importance of IDS in securing Open RAN networks cannot be overstated. It serves as a cornerstone in the establishment of robust security frameworks essential for the sustainable growth and widespread adoption of Open RAN architectures. Moving forward to advanced security, we provided a insights on new technologies such as blockchain, AI/ML, LLM that could support a secure Open RAN as new threats emerge, with insights on future research directions.

REFERENCES

[1] I-Security Agency, *Open Radio Access Network Security Considerations*, Nat. Secur. Agency (NSA), Cybersecur. Infrastruct. Secur. Agency (CISA), USA, 2022.

[2] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open RAN security: Challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 214, May 2023, Art. no. 103621.

[3] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in *Proc. IEEE Conf. Standards for Commun. Netw. (CSCN)*, Sep. 2017, pp. 193–199.

[4] D. Attanayaka, P. Porambage, M. Liyanage, and M. Ylianttila, "Peer-to-peer federated learning based anomaly detection for open radio access networks," in *Proc. IEEE Int. Conf. Commun.*, May 2023, pp. 5464–5470.

[5] T. Sundqvist, M. Bhuyan, and E. Elmroth, "Robust procedural learning for anomaly detection and observability in 5G RAN," *IEEE Trans. Netw. Service Manag.*, vol. 21, no. 2, pp. 1432–1445, Apr. 2024.

[6] Z. Mahrez, M. B. Driss, E. Sabir, W. Saad, and E. Driouch, "Benchmarking of anomaly detection techniques in O-RAN for handover optimization," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2023, pp. 119–125.

[7] O. T. Basaran, M. Basaran, D. Turan, H. G. Bayrak, and Y. S. Sandal, "Deep autoencoder design for RF anomaly detection in 5G O-RAN near-RT RIC via xApps," in *Proc. IEEE Int. Conf. Commun. Workshops*, May 2023, pp. 549–555.

[8] S. Sonawane, S. Karsoliya, P. Saurabh, and B. Verma, "Self configuring intrusion detection system," in *Proc. 4th Int. Conf. Comput. Intell. Commun. Netw.*, Nov. 2012, pp. 757–761.

[9] O. Orhan, V. N. Swamy, T. Tetzlaff, M. Nassar, H. Nikopour, and S. Talwar, "Connection management xAPP for O-RAN RIC: A graph neural network and reinforcement learning approach," in *Proc. 20th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2021, pp. 936–941.

[10] D. Dik and M. S. Berger, "Open-RAN fronthaul transport security architecture and implementation," *IEEE Access*, vol. 11, pp. 46185–46203, 2023.

[11] S. Vasanthi and S. Chandrasekar, "A study on network intrusion detection and prevention system current status and challenging issues," in *Proc. 3rd Int. Conf. Adv. Recent Technol. Commun. Comput. (ARTCom)*. IET, 2011, pp. 181–183.

[12] D. Dik and M. S. Berger, "Transport security considerations for the open-RAN fronthaul," in *Proc. IEEE 4th 5G World Forum (5GWF)*, Oct. 2021, pp. 253–258.

[13] M. K. Motalleb, V. Shah-Mansouri, S. Parsaeefard, and O. L. A. López, "Resource allocation in an open RAN system using network slicing," *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 1, pp. 471–485, Mar. 2023.

[14] D. Mimran, R. Bitton, Y. Kfir, E. Klevansky, O. Brodt, H. Lehmann, Y. Elovici, and A. Shabtai, "Security of open radio access networks," *Comput. Secur.*, vol. 122, Nov. 2022, Art. no. 102890.

[15] E. Amiri, N. Wang, M. Shojafar, and R. Tafazolli, "Optimizing virtual network function splitting in open-RAN environments," in *Proc. IEEE 47th Conf. Local Comput. Netw. (LCN)*, Sep. 2022, pp. 422–429.

[16] V. Q. Rodriguez, F. Guillemin, A. Ferrieux, and L. Thomas, "Cloud-RAN functional split for an efficient fronthaul network," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 245–250.

[17] O-RAN, *O-RAN Work Group 1 (Use Cases and Overall Architecture) Use Cases Analysis Report*, AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, Orange, O-RAN Alliance, Germany, 2023, pp. 1–83.

[18] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1376–1411, 2nd Quart., 2023.

[19] P. V. Alves, M. A. Goldbarg, W. K. Barros, I. D. Rego, J. V. Filho, A. M. Martins, V. A. De Sousa Jr., R. D. R. Fontes, E. H. D. S. Aranha, A. V. Neto, and M. A. C. Fernandes, "Machine learning applied to anomaly detection on 5G O-RAN architecture," *Proc. Comput. Sci.*, vol. 222, pp. 81–93, Jan. 2023.

[20] H. Liu, J. Zong, Q. Wang, Y. Liu, and F. Yang, "Cloud native based intelligent RAN architecture towards 6G programmable networking," in *Proc. 7th Int. Conf. Comput. Commun. Syst. (ICCCS)*, Apr. 2022, pp. 623–627.

[21] S. Lagén, L. Giupponi, A. Hansson, and X. Gelabert, "Modulation compression in next generation RAN: Air interface and fronthaul tradeoffs," *IEEE Commun. Mag.*, vol. 59, no. 1, pp. 89–95, Jan. 2021.

[22] T. Specification, *O-RAN Work Group 11 (Security Work Group) Security Protocols Specifications*, AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, Orange, O-RAN Alliance, Germany, 2023.

[23] T. Specification, *O-RAN Working Group 11 (Security Working Group) Security Requirements Specifications*, AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, Orange, O-RAN Alliance, Germany, 2022.

[24] ORAN Alliance. (2020). *O-RAN Use Cases and Deployment Scenarios: Towards Open and Smart RAN*. [Online]. Available: https://www.o-ran.org/resources

[25] Report, *O-RAN Security Focus Group (SFG) Study on Security for Non-RT-RIC O-RAN Security Focus Group (SFG) Study on Security for Non-RT-RIC*, AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, Orange, O-RAN Alliance, Germany, 2022.

[26] *O-RAN Work Group 1 (Use Cases and Overall Architecture) Use Cases Detailed Specification*, AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, Orange, O-RAN Alliance, Germany, 2023.

[27] M. A. Habib, H. Zhou, P. E. Iturria-Rivera, M. Elsayed, M. Bavand, R. Gaigalas, Y. Ozcan, and M. Erol-Kantarci, "Intent-driven intelligent control and orchestration in O-RAN via hierarchical reinforcement learning," 2023, *arXiv:2307.02754*.

[28] B. Balasubramanian, E. S. Daniels, M. Hiltunen, R. Jana, K. Joshi, R. Sivaraj, T. X. Tran, and C. Wang, "RIC: A RAN intelligent controller platform for AI-enabled cellular networks," *IEEE Internet Comput.*, vol. 25, no. 2, pp. 7–17, Mar. 2021.

[29] (2020). *The Innovation Potential of Non Real-Time RAN Intelligent Controller*. [Online]. Available: https://www.ericsson.com/en/blog/2020/10/innovation-potential-of-non-real-time-ran-intelligent-controller

[30] G. M. Almeida, G. Z. Bruno, A. Huff, M. Hiltunen, E. P. Duarte, C. B. Both, and K. V. Cardoso, "RIC-O: Efficient placement of a disaggregated and distributed RAN intelligent controller with dynamic clustering of radio nodes," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 2, pp. 446–459, Feb. 2024.

[31] A. Chiejina, B. Kim, K. Chowhdury, and V. K. Shah, "System-level analysis of adversarial attacks and defenses on intelligence in O-RAN based cellular networks," 2024, *arXiv:2402.06846*.

[32] M. Hoffmann and P. Kryszkiewicz, "Signaling storm detection in IIoT network based on the open RAN architecture," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops*, May 2023, pp. 1–2.

[33] D. Sabella, A. de Domenico, E. Katranaras, M. A. Imran, M. di Girolamo, U. Salim, M. Lalam, K. Samdanis, and A. Maeder, "Energy efficiency benefits of RAN-as-a-service concept for a cloud-based 5G mobile network infrastructure," *IEEE Access*, vol. 2, pp. 1586–1597, 2014.

[34] Report, *O-RAN Work Group 11 (Security Working Group) O-RAN Security Threat Modeling and Risk Assessment*, AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, Orange, O-RAN Alliance, Germany, 2023, pp. 1–129.

[35] Report, *O-RAN Working Group 11 (Security Work Group) Study on Security Log Management*, AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, Orange, O-RAN Alliance, Germany, 2023, pp. 1–27.

[36] Report, *O-RAN Work Group 11 (Security Work Group) Study on Security for O-Cloud*, AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, Orange, O-RAN Alliance, Germany, 2023.

[37] Report, *O-RAN Work Group 11 (Security Work Group) Study on Security for Near Real Time RIC and xApps*, AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, Orange, O-RAN Alliance, Germany, 2023.

[38] J.-H. Huang, S.-M. Cheng, R. Kaliski, and C.-F. Hung, "Developing xApps for rogue base station detection in SDR-enabled O-RAN," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops*, May 2023, pp. 1–6.

[39] B. Brik, K. Boutiba, and A. Ksentini, "Deep learning for B5G open radio access network: Evolution, survey, case studies, and challenges," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 228–250, 2022.

[40] M. A. Habibi, M. Nasimi, B. Han, and H. D. Schotten, "A comprehensive survey of RAN architectures toward 5G mobile communication system," *IEEE Access*, vol. 7, pp. 70371–70421, 2019.

[41] J. Groen, S. Doro, U. Demir, L. Bonati, M. Polese, T. Melodia, and K. Chowdhury, "Implementing and evaluating security in O-RAN: Interfaces, intelligence, and platforms," 2023, *arXiv:2304.11125*.

[42] O. Alliance. *O-RAN Security Threat Modeling and Remediation Analysis*, Tech. Specification, O-RAN SFG, Secur. Focus Group, O-RAN. SFG. Threat-Model-v03. 00, AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, Orange, O-RAN Alliance, Germany, 2022.

[43] C. Nobles, "Botching human factors in cybersecurity in business organizations," *HOLISTICA-J. Bus. Public Admin.*, vol. 9, no. 3, pp. 71–88, Dec. 2018.

[44] *Evolving to a Strong Cloud RAN Security Posture Minimizing Threats to 5G Cloud RAN Critical Infrastructure*, Ericsson, Stockholm, Sweden, 2022. [Online]. Available: https://www.ericsson.com/4ae608/assets/local/ran/doc/evolving-strong-cloud-ran-security-posture-report.pdf

[45] F. Tian, P. Zhang, and Z. Yan, "A survey on C-RAN security," *IEEE Access*, vol. 5, pp. 13372–13386, 2017.

[46] S. Soltani, M. Shojafar, A. Brighente, M. Conti, and R. Tafazolli, "Poisoning bearer context migration in O-RAN 5G network," *IEEE Wireless Commun. Lett.*, vol. 12, no. 3, pp. 401–405, Mar. 2023.

[47] S. Haas, M. Hasler, F. Pauls, S. Köpsell, N. Asmussen, M. Roitzsch, and G. Fettweis, "Trustworthy computing for O-RAN: Security in a latency-sensitive environment," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2022, pp. 826–831.

[48] E. Habler, R. Bitton, D. Avraham, D. Mimran, E. Klevansky, O. Brodt, H. Lehmann, Y. Elovici, and A. Shabtai, "Adversarial machine learning threat analysis and remediation in open radio access network (O-RAN)," 2022, *arXiv:2201.06093*.

[49] M. K. Motalleb, C. Benzaïd, T. Taleb, and V. Shah-Mansouri, "Moving target defense based secured network slicing system in the O-RAN architecture," 2023, *arXiv:2309.13444*.

[50] G. Carrozzo, M. S. Siddiqui, A. Betzler, J. Bonnet, G. M. Perez, A. Ramos, and T. Subramanya, "AI-driven zero-touch operations, security and trust in multi-operator 5G networks: A conceptual architecture," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2020, pp. 254–258.

[51] C. Benzaid and T. Taleb, "AI-driven zero touch network and service management in 5G and beyond: Challenges and research directions," *IEEE Netw.*, vol. 34, no. 2, pp. 186–194, Mar. 2020.

[52] C. Benzaid and T. Taleb, "ZSM security: Threat surface and best practices," *IEEE Netw.*, vol. 34, no. 3, pp. 124–133, May 2020.

[53] E. Coronado, R. Behravesh, T. Subramanya, A. Fernàndez-Fernàndez, M. S. Siddiqui, X. Costa-Pérez, and R. Riggio, "Zero touch management: A survey of network automation solutions for 5G and 6G networks," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2535–2578, 4th Quart., 2022.

[54] S. Sengupta, T. Chakraborti, and S. Kambhampati, "MTDeep: Boosting the security of deep neural nets against adversarial attacks with moving target defense," in *Proc. Workshops 32nd AAAI Conf. Artif. Intell.*, in Lecture Notes in Computer Science, vol. 11836. Cham, Switzerland: Springer, 2019, pp. 479–491.

[55] V. Theodorou, A. Lekidis, T. Bozios, K. Meth, A. Fernández-Fernández, J. Tavlor, P. Diogo, P. Martins, and R. Behravesh, "Blockchain-based zero touch service assurance in cross-domain network slicing," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Jun. 2021, pp. 395–400.

[56] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[57] W. Tiberti, E. Di Fina, A. Marotta, and D. Cassioli, "Impact of man-in-the-middle attacks to the O-RAN inter-controllers interface," in *Proc. IEEE Future Netw. World Forum (FNWF)*, Oct. 2022, pp. 367–372.

[58] P. Kryszkiewicz and M. Hoffmann, "Open RAN for detection of a jamming attack in a 5G network," in *Proc. IEEE 97th Veh. Technol. Conf. (VTC-Spring)*, Florence, Italy. New York, NY, USA: Institute of Electrical and Electronics Engineers, Jun. 2023, pp. 1–2.

[59] J. Snehi, M. Snehi, A. Bhandari, V. Baggan, and R. Ahuja, "Introspecting intrusion detection systems in dealing with security concerns in cloud environment," in *Proc. 10th Int. Conf. Syst. Model. Advancement Res. Trends (SMART)*, Dec. 2021, pp. 345–349.

[60] C.-F. Hung, Y.-R. Chen, C.-H. Tseng, and S.-M. Cheng, "Security threats to xApps access control and E2 interface in O-RAN," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 1197–1203, 2024.

[61] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3GPP 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 170–195, 1st Quart., 2020.

[62] C.-H. Tseng, C.-F. Hung, B.-K. Hong, and S.-M. Cheng, "On manipulating routing table to realize redirect attacks in O-RAN by malicious xApp," in *Proc. 26th Int. Symp. Wireless Pers. Multimedia Commun. (WPMC)*, Nov. 2023, pp. 288–292.

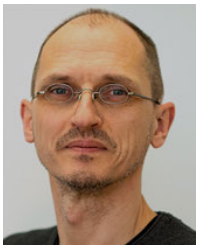
[63] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020.

[64] R. Harrilal-Parchment, I. F. Pujol, and K. Akkaya, "Performance evaluation of quantum-resistant open fronthaul communications in 5G," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2023, pp. 1–6.
[65] M. Sjoholmsierchio, B. Hale, D. Lukaszewski, and G. Xie, "Strengthening SDN security: Protocol dialecting and downgrade attacks," in *Proc. IEEE 7th Int. Conf. Netw. Softwarization (NetSoft)*, Jun. 2021, pp. 321–329.
[66] K. Bhargavan, C. Brzuska, C. Fournet, M. Green, M. Kohlweiss, and S. Zanella-Béguelin, "Downgrade resilience in key-exchange protocols," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 506–525.
[67] M. Z. Neto, G. A. A. Santana, F. Sapata, M. Munoz, A. M. S. P. Moraes, T. Morais, and D. L. Goldfarb, *Cloud Security Principles and Frame*. USA: Sybex, Jan. 2021, pp. 39–63.
[68] Amazon Web Services (AWS), *Introduction to DevOps on AWS*, Seattle, WA, USA, 2020.
[69] D. Brake, "A U.S. national strategy for 5G and future wireless innovation," Inf. Technol. Innov. Found., Apr. 2020. [Online]. Available: https://itif.org/publications/2020/04/27/us-national-strategy-5g-and-future-wireless-innovation
[70] J. Boyens, C. Paulsen, R. Moorthy, N. Bartol, and S. A. Shankles, "Supply chain risk management practices for federal information systems and organizations," *NIST Special Publication*, vol. 800, no. 161, p. 32, 2015.
[71] C. Balding, "Revisiting the United States telecommunications network policy in a post-Huawei world: Improving economic competitiveness, addressing security weakness, and building alliances," New Kite Data Labs, USA, Jun. 2021. [Online]. Available: https://ssrn.com/abstract=3861826
[72] A. Mehrban and M. Jani, "Securing OPEN-RAN equipment using blockchain-based supply chain verification," 2024, *arXiv:2402.17632*.
[73] N. Islam, F. Monir, M. M. Mahbubul Syeed, M. Hasan, and M. F. Uddin, "Federated learning integration in O-RAN: A concise review," in *Proc. 33rd Int. Telecommun. Netw. Appl. Conf.*, Nov. 2023, pp. 283–288.
[74] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2671–2701, 3rd Quart., 2019.
[75] S. Walling and S. Lodh, "A survey on intrusion detection systems: Types, datasets, machine learning methods for NIDS and challenges," in *Proc. 13th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Oct. 2022, pp. 1–7.
[76] S. M. Othman, N. T. Alsohybe, F. M. Ba-Alwi, and A. T. Zahary, "Survey on intrusion detection system types," *Int. J. Cyber-Secur. Digital Forensics*, vol. 7, pp. 444–462, Dec. 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:198363928
[77] R. Jain and S. Paul, "Network virtualization and software defined networking for cloud computing: A survey," *IEEE Commun. Mag.*, vol. 51, no. 11, pp. 24–31, Nov. 2013.
[78] A. Garcia-Saavedra and X. Costa-Pérez, "O-RAN: Disrupting the virtualized RAN ecosystem," *IEEE Commun. Standards Mag.*, vol. 5, no. 4, pp. 96–103, Dec. 2021.
[79] G. Garcia-Aviles, A. Garcia-Saavedra, M. Gramaglia, X. Costa-Perez, P. Serrano, and A. Banchs, "Nuberu: Reliable RAN virtualization in shared platforms," in *Proc. 27th Annu. Int. Conf. Mobile Comput. Netw.*, Oct. 2021, pp. 749–761.
[80] S. K. Singh, R. Singh, and B. Kumbhani, "The evolution of radio access network towards open-RAN: Challenges and opportunities," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Apr. 2020, pp. 1–6.
[81] B. Hanselman, "Security benefits of open virtualized RAN," 451 Res. Market (S&P Global Market Intell.), Pathfinder Rep., 2020, pp. 1–13. Accessed: Feb. 3, 2024. [Online]. Available: https://www.cisco.com/c/dam/en/us/solutions/service-provider/pdfs/5g-network-architecture/white-paper-sp-open-vran-security-benefits.pdf
[82] A. S. Abdalla, P. S. Upadhyaya, V. K. Shah, and V. Marojevic, "Toward next generation open radio access networks: What O-RAN can and cannot do!" *IEEE Netw.*, vol. 36, no. 6, pp. 206–213, Nov. 2022.
[83] D. Abecassis, M. Kende, S. Osman, R. Dhamija, and A. Sethi, "Report for the telecom infra project the economic impact of open and disaggregated technologies and the role of tip in India," Analysys Mason, London, U.K., Jul. 2021, pp. 1–20.
[84] (2024). *5G Security Solutions in Open RAN*. [Online]. Available: https://networkblog.global.fujitsu.com/2023/03/24/5g-security-solutions-in-open-ran/
[85] P. Fetterolf. *The Economic Benefits of Open RAN Technology*. Accessed: Feb. 9, 2024. [Online]. Available: https://docs.o-ran-sc.org/en/latest/architecture/architecture.html
[86] C. Gabriel and R. Kompany, "Open RAN: Ready for prime time?" Analysys Mason, London, U.K., Apr. 2021.
[87] A. Scalingi, S. D'Oro, F. Restuccia, T. Melodia, and D. Giustiniano, "Det-RAN: Data-driven cross-layer real-time attack detection in 5G open RANs," in *Proc. IEEE Int. Conf. Comput. Commun.*, May 2024, pp. 1–10.
[88] Open RAN Policy Coalition. (2021). *Open RAN Security in 5G*. [Online]. Available: https://www.openranpolicy.org/how-open-ran-can-bring-security-advantages/
[89] NTIA, "Open RAN security report may," Definitive Guide Open RAN Secur., Rakuten Symphony, Oct. 2022, vol. 103, no. 3, pp. 40–49.
[90] X. Krasniqi, E. Hajrizi, and B. Qehaja, "Challenges and lessons learned during private 5G open RAN deployments," in *Proc. 3rd Int. Conf. Electr., Comput., Commun. Mechatronics Eng. (ICECCME)*, Jul. 2023, pp. 1–6.
[91] JTCIJSS. *Information Technology–Security Techniques–Information Secur. Manage. Systems–Requirements*. Standard ISO/IEC 27, 2013.
[92] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture, special publication (NIST SP)," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Special Publication 800-207, 2020. Accessed: Jun. 3, 2024. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420, doi: 10.6028/NIST.SP.800-207.
[93] *Security Guidance for 5G Cloud Infrastructures Part I*, Nat. Secur. Agency, 2021.
[94] M. Negreiro. (Feb. 2023). *The NIS2 Directive—A High Common Level of Cybersecurity in the EU*. European Parliamentary Research Service. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf
[95] M. Rice and D. Ph, "National center," White House, Washington, DC, USA, Mar. 2023.
[96] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN," *Comput. Netw.*, vol. 217, Nov. 2022, Art. no. 109358.
[97] S. Nakamoto and A. Bitcoin. (2008). *A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[98] H. Xu, L. Zhang, and Y. Sun, "BE-RAN: Blockchain-enabled open RAN with decentralized identity management and privacy-preserving communication," 2021, *arXiv:2101.10856*.
[99] W. Tong, X. Dong, Y. Shen, and J. Zheng, "BC-RAN: Cloud radio access network enabled by blockchain for 5G," *Comput. Commun.*, vol. 162, pp. 179–186, Oct. 2020.
[100] N. Aryal, F. Ghaffari, E. Bertin, and N. Crespi, "Moving towards open radio access networks with blockchain technologies," in *Proc. 5th Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Oct. 2023, pp. 1–9.
[101] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102693.
[102] X. Ling, J. Wang, Y. Le, Z. Ding, and X. Gao, "Blockchain radio access network beyond 5G," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 160–168, Dec. 2020.

EMMANUEL N. AMACHAGHI (Graduate Student Member, IEEE) is currently a Researcher at the 5G/6G Innovation Centre (5GIC & 6GIC), Institute for Communication Systems (ICS), University of Surrey, U.K. He is a Chartered Engineer with an impressive industry track record spanning over 20 years in the information technology and telecommunications sectors. Throughout his career, he has collaborated with industry giants such as Cisco, Vodafone, Orange, and numerous other Mobile Network Operators (MNOs) worldwide. He reviews academic paper in the IEEE International Conference on Communications, IEEE Wireless Communications, and the *International Journal of Communication Systems*. His research interests include security in Open RAN and vehicular networks (V2X), machine learning, and blockchain applications for wireless communication systems.

MOHAMMAD SHOJAFAR (Senior Member, IEEE) received the Ph.D. degree (Hons.) in ICT from the Sapienza University of Rome, Rome, Italy, in 2016. He is currently a Senior Lecturer (an Associate Professor) of network security and an Intel Innovator with the 5G/6G Innovation Centre (5G/6GIC), Institute for Communication Systems, University of Surrey, U.K. Before joining 5G/6GIC, he was a Senior Researcher and a Marie Curie Fellow with the SPRITZ Security and Privacy Research Group, University of Padua, Italy. He secured around £1.9M as PI in various EU/UK projects, including ORAN-TWIN (funded by EPSRC/DSIT CHEDDAR Hub UK; 2024), D-XPERT (funded by I-UK/UK;2024), 5G MoDE (funded by DSIT/UK;2023), 5G ONE4HDD (funded by DSIT/UK;2023), TRACE-V2X (funded by EU/MSCA-SE;2023), AUTOTRUST (funded by ESA/EU;2021), PRISEN-ODE (funded by EU/MSCA-IF:2019), and SDN-Sec (funded by Italian Government:2018). He was also COI of various UK/EU projects like HiPER-RAN (funded by DSIT/UK;2023), APTd5G project (funded by EPSRC/UKI-FNI:2022), ESKMARALD (funded by UK/NCSC;2022), GAUChO, S2C and SAMMClouds (funded by Italian Government;2016-2018). He was also a COI of various U.K./EU projects, such as HiPER-RAN (funded by DSIT/U.K., 2023), APTd5G Project (funded by EPSRC/UKI-FNI, 2022), ESKMARALD (funded by U.K./NCSC, 2022), GAUChO, S2C, and SAMMClouds (funded by Italian Government, 2016–2018). He is a Professional ACM Member, an ACM Distinguished Speaker, a fellow of the Higher Education Academy, and a Marie Curie Alumni. He is an Associate Editor of IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, and *Computer Networks*.

CHUAN HENG FOH (Senior Member, IEEE) received the M.Sc. degree from Monash University, Melbourne, VIC, Australia, in 1999, and the Ph.D. degree from The University of Melbourne, Melbourne, in 2002. After the Ph.D. degree, he spent six months as a Lecturer with Monash University. In December 2002, he joined Nanyang Technological University, Singapore, as an Assistant Professor, until 2012. He is currently a Senior Lecturer with the University of Surrey, Guildford, U.K. He has authored or coauthored more than 180 refereed papers in international journals and conferences. His research interests include protocol design, machine learning application, and performance analysis of various computer networks, including wireless local area networks, mobile ad hoc and sensor networks, vehicular networks, the Internet of Things, 5G/6G networks, and Open RAN. He served as the Vice Chair (Europe/Africa) for IEEE TCGCC, from 2015 to 2017. He is currently the Vice-Chair of the IEEE VTS Ad Hoc Committee on Mission Critical Communications. He is on the editorial boards of several international journals.



KLAUS MOESSNER (Senior Member, IEEE) is currently a Professor of communications engineering with the University of Technology Chemnitz and a Professor of cognitive networks with the Institute for Communication Systems and the 5G Innovation Centre, University of Surrey. He was involved in many projects in cognitive communications, service provision, and the IoT. He was responsible for the work on cognitive decision-making mechanisms in the CR Project ORACLE. He led the work on radio awareness in the ICT FP7 Project QoSMOS and led the H2020 Speed5G Project. He led the EU-Taiwan Project Clear5G, investigating the extensions of 5G systems needed to serve the particular requirements of future factories. His research interests include cognitive networks, the IoT deployments, sensor data-based knowledge generation, reconfiguration, and resource management. He was the Founding Chair of the IEEE DYSPAN Working Group (WG6) on Sensing Interfaces for Future and Cognitive Communication Systems.