Received 1 May 2024; revised 21 June 2024; accepted 15 July 2024. Date of publication 18 July 2024; date of current version 8 January 2025.

Digital Object Identifier 10.1109/OJCOMS.2024.3430823

Open RAN: A Concise Overview

MOHAMAD SAALIM WANI [1], MATHIAS KRETSCHMER [1], BERND SCHRÖDER [2], ANDREAS GREBE [3] (Member, IEEE), AND MICHAEL RADEMACHER [4,5]

[1]Department of Cooperation Systems, Fraunhofer FIT, 53757 Sankt Augustin, Germany
[2]Department of Industrial Communication & Data Research, brown-iposs GmbH, 53229 Bonn, Germany
[3]Institute on Computer and Communication Technology, Technische Hochschule Köln, 50679 Cologne, Germany
[4]Department of Computer Science, Hochschule Bonn-Rhein-Sieg, 53757 Sankt Augustin, Germany
[5]Department of Cyber Analysis & Defense, Fraunhofer FKIE, 53177 Bonn, Germany

CORRESPONDING AUTHOR: M. S. WANI (e-mail: mohamad.saalim.wani@fit.fraunhofer.de)

This work was supported by the Federal Ministry for Digital and Transport of the Federal Republic of Germany (Förderkennzeichen, IndustrieStadtpark: 5G-Anwendungen im Projektgebiet IndustrieStadtpark Troisdorf) under Grant 165GU054B.

ABSTRACT Open RAN has emerged as a transformative approach in the evolution of cellular networks, addressing challenges posed by modern applications and high network density. By leveraging disaggregated, virtualized, and software-based elements interconnected through open standardized interfaces, Open RAN introduces agility, cost-effectiveness, and enhanced competition in the Radio Access Network (RAN) domain. The Open RAN paradigm, driven by the O-RAN Alliance specifications, is set to transform the telecom ecosystem. Despite extensive technical literature, there is a lack of succinct summaries for industry professionals, researchers, and policymakers. This paper addresses this gap by providing a concise, yet comprehensive overview of Open RAN. Compared to previous work, our approach introduces Open RAN by gradually splitting up different components known from previous RAN architectures. We believe that this approach leads to a better understanding for people already familiar with the general concept of mobile communication networks. Building upon this general understanding of Open RAN, we introduce key architectural principles, interfaces, components and use-cases. Moreover, this work investigates potential security implications associated with adopting Open RAN architecture, emphasizing the necessity of robust network protection measures.

INDEX TERMS Open RAN, 5G, security, mobile networks.

I. INTRODUCTION

CELLULAR networks are becoming ever more complex with the advent of innovative technologies such as Network Slicing [1], [2], Massive Multiple-Input Multiple-Output (MIMO) [3], Multi-Band and Multi-Technology support, Millimeter wave, and Machine Learning-based developments [4], [5], [6]. Additionally, the expected surge in both data volume and diversity further contributes to the growing complexity of these networks [7]. Network operators are under pressure to keep up with the market trends by encompassing newer technologies, continuously upgrading and maintaining their networks while keeping the cost per bit as low as possible. To reduce expenses and simultaneously roll out more advanced technology solutions, mobile operators have begun to investigate new revenue-generating services.

Recently, the Core Network has seen significant changes with the advent of Software Defined Networking (SDN) and Network Functions Virtualization (NFV) [8], [9], enabling the operators to build a more agile and less expensive core [10]. However, the Radio Access Network (RAN) which involves major costs in building mobile networks, has remained relatively untouched in terms of achieving cost-effectiveness, despite experiencing notable advancements. It is estimated that approximately 65–70% of the total cost of owning and operating a mobile network is attributed to the RAN [7]. Thus, there is a clear and pressing need for a similar revolution in the RAN domain to establish a well-balanced and economically sustainable network ecosystem.

Most RAN deployments worldwide still rely on monolithic integrated solutions based on proprietary hardware and software. These systems typically feature undisclosed interfaces,

leading to vendor lock-in where operators must continue with the same vendor's equipment throughout their network deployment. This dependency on specific vendors poses supply chain risks; disruptions or stagnations in procurement can render services inoperable.

The RAN equipment domain is currently dominated by a few vendors [11] and seen by the network operators as black boxes lacking transparency. These systems often lack advanced data-driven optimization and closed-loop control capabilities needed to manage complex, heterogeneous networks effectively. Even vendor-specific closed-loop optimization techniques provide minimal operator control, impacting service quality for customers.

In order to overcome these limitations, research and standardization initiatives have envisioned Open RAN as the RAN of the future. Open RAN deployments are built on disaggregated, virtualized, software-based elements that are linked by open standardized interfaces and could be orchestrated using intelligent controllers. It envisions to bring cloud-scale economics and introduce agility in the RAN. Virtualization and disaggregation allow for flexible deployments based on cloud-native concepts. This improves the RAN's resilience and reconfigurability. Open standardized interfaces would allow RAN deployments to be multi-vendor and allow small-scale vendors to enter the RAN development market, enabling a more competitive and vibrant supplier system. Intelligent controllers leveraging open interfaces can significantly enhance network automation, making RAN optimization more efficient, self-driven, cost-effective, and accessible for network operators.

In order to benefit most from this work, it is important to distinguish between the following terms: Open RAN, O-RAN, and OpenRAN. The term Open RAN refers to the movement in mobile networks towards building a disaggregated RAN functionality by employing open interfaces between its elements. O-RAN, the second term, is affiliated with the O-RAN Alliance, the organization responsible for the development of the O-RAN architecture [12]. The architecture developed by O-RAN Alliance serves as the fundamental framework for this paper. In contrast, the term OpenRAN (written as one word) is associated with a project group established by TIP (Telecom Infra Project[1]) but holds no relevance in the context of this work.

II. RELATED WORK

Open RAN has garnered significant attention in the mobile networks industry in recent years, with numerous private companies and research groups actively advancing the idea. The rising interest in Open RAN has facilitated numerous real-world deployments, which continue to expand over time [13]. Moreover, the growing interest in Open RAN has also resulted in several research articles. Some of these publications provide detailed tutorials on various aspects of Open RAN.

One comprehensive survey paper [14] on Open RAN development covers a wide range of topics, including its evolution, state-of-the-art technologies, related projects, ongoing activities, and future research directions. It also delves into the O-RAN architecture components and discusses security in the O-RAN architecture. Another in-depth tutorial paper [15] explores O-RAN specifications, describing its architecture, design principles, and interfaces, and addressing innovations and challenges, including AI and ML workflows, security threats, and standardization issues. A third tutorial [10] covers topics such as O-RAN architecture, use cases, deployment aspects, open-source projects, open issues, challenges, and future research directions, with a brief discussion on O-RAN security. Other research articles focus on specific facets of Open RAN, such as machine learning aspects [16], security concerns [11], [12], [17], [18], [19], [20], [21], capabilities and limitations [22], open-source software suitable for deploying Open RAN [23], [24], and use-cases of Open RAN [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38]. Additionally, companies involved in Open RAN have released numerous white papers on the subject [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49].

Despite these extensive studies, there is a lack of a short, concise introduction aimed at readers with a general understanding of mobile networks, in particular providing a comprehensive overview of the security landscape. While the existing survey papers focus on O-RAN risks, they do not compare these risks with those of traditional RAN. To gain a broader understanding of O-RAN risks, it is essential to contrast them with those associated with traditional RAN, thus broadening the perspective offered by the existing survey papers.

This article aims to address these gaps by offering a concise yet comprehensive overview of Open RAN, systematically introducing the O-RAN concept and its security aspects. Unlike most papers that present O-RAN without contextualizing it within the 5G RAN framework, this paper demystifies Open RAN by illustrating how additional components integrate with the 5G architecture to form the O-RAN architecture. We also provide information about security protocols implemented in each new O-RAN interface, which is often missing in the literature and the aforementioned survey papers. Regarding security, we first present the security risks of the O-RAN architecture, including those common to 5G RAN, then briefly compare O-RAN with 5G RAN in terms of security, and finally provide insights into risks unique to O-RAN due to the introduction of novel components and interfaces.

III. BACKGROUND

A. MOBILE NETWORK ARCHITECTURE

A mobile network architecture can be divided into three components: User Equipment (UE)s, the RAN, and the Core Network as shown in Fig. 1. Those three main components of a mobile network are briefly described below.

[1] https://telecominfraproject.com

FIGURE 1. A simple overview about the basic components of a mobile network. This overview will be further specified in the following.

FIGURE 2. An overview of the evolution of the RAN in mobile networks.

The **UE** is a device the end-user uses to communicate with the mobile network (e.g., a smartphone).Typically, it is authenticated into the network using a Subscriber Identity Module (SIM) Card.

The **RAN** consists of Base Stations (BSs) and is used to facilitate communication between the UE and the core network via radio connectivity. The main task of the RAN is radio resource management. Each BS typically includes a Radio Unit (RU) with RF circuitry for signal transmission and reception, and a Baseband Unit (BBU) which handles computational tasks like radio management and resource allocation.

The **Core Network** is the central component of a mobile network, responsible for a wide range of functions, including access management, mobility support, and the provision of essential services such as interconnectivity.

B. EVOLUTION OF THE RAN

Over the past three decades, base stations have transformed from being monolithic devices with proprietary hardware, software, and interfaces to disaggregated instanciations using Commercial Off-the-Shelf (COTS) hardware. The following section briefly explains various types of Base Stations (BSs).

Decentralized RAN (D-RAN): In the D-RAN concept, both the RU and BBU are co-located at the cell site, with all processing done locally. The BBU is typically placed in an air-conditioned shelter, while the RU (or Remote Radio Unit (RRU) when near the antenna) is either in the same room or at the top of the tower. The BBU functions as proprietary software on specialized hardware, and the RRU is also proprietary. As the number of UEs increases, more BS are required, raising costs for space and cooling.

Centralized-RAN (C-RAN): To reduce overall expenditures, the C-RAN architecture was introduced. In C-RAN, BBUs from several base stations are centralized, minimizing site rental and Operation and Maintenance (OAM) efforts [50]. New RRUs can be added without setting up new BBU at the cell site, thus addressing growing traffic demands without significantly increasing costs. Similar to D-RAN, the BBU, RRU, and Fronthaul (FH) interface remain proprietary. However, C-RAN's limitations include high FH capacity requirements, single points of failure, and vendor lock-in, making it suitable primarily for urban scenarios.

Virtualized-RAN (vRAN) is an enhanced version of C-RAN. In vRAN, proprietary BBU hardware is replaced with COTS servers, and software is decoupled from hardware using NFV principles. This enables network functions to run on virtual machines or containers on top of COTS hardware, although the interface between COTS-based BBUs and RRUs remains proprietary [51]. Virtualizing BBU pools allows for resource sharing among multiple sites, potentially reducing data processing needs by approximately 50% [14]. However, the increased network complexity makes resource sharing among radio nodes challenging.

IV. OPEN RAN

The transition from vRAN to Open RAN involves standardizing interfaces between RAN components while incorporating cloud-based aspects from vRAN. One of the key interfaces standardized/opened by Open RAN is the Open FH between RRU and BBU [51]. This framework also enables the separation of the traditional Baseband Unit into Distributed Unit (DU) and Central Unit (CU). By adopting standardized interfaces, Open RAN promotes multi-vendor deployments, empowering operators to mix and match components such as RUs, DUs, and CUs to tailor solutions for diverse deployment scenarios [40]. Additionally, Open RAN supports replacing proprietary RRU hardware with COTS-based Software Defined Radio (SDR) [51]. Moreover, it enables decoupling the RAN control plane from the user plane and integrating data-driven intelligence to automate complex RAN management tasks [7].

A. KEY OPEN RAN GROUPS

The following section briefly introduces the working of two main groups leading the Open RAN movement.

The **O-RAN Alliance** was founded in 2018 with the intention of promoting openness and intelligence in the RAN after the two organizations C-RAN alliance and the X-RAN forum joined forces [52]. Since its launch, the O-RAN alliance has quickly scaled up and currently has more than 300 members and contributors. The major goal of the O-RAN alliance is to standardize an architecture and set of interfaces for the Open RAN paradigm. The alliance defines the **O-RAN architecture** and specifications to extend the RAN standards to include openness and intelligence. It also focuses on developing reference open-source software and hardware for various O-RAN components. Additionally, it provides guidance to the members of the alliance to test the inter-working of O-RAN solutions they develop. The O-RAN alliance is more focused on 4G and 5G networks compared to Telecom Infra Project (TIP) which also covers aspects beyond the RAN [51].

The specification tasks of the O-RAN Alliance are divided into several Working Groups (WG)s as shown in Table 2. As discussed earlier, this paper is focused towards the O-RAN architecture.

TIPs was founded in 2016 with the objective of providing universal Internet access. It follows an engineering-oriented

TABLE 1. Comparison of different types of RAN.

Types	BBU hardware	BBU Software	Vendor-lockin	Virtualization	RAN Intelligent Controller (RIC)
D-RAN	Proprietary H/w	Proprietary S/w	Yes	No	No
C-RAN	Proprietary H/w	Proprietary S/w	Yes	No	No
vRAN	COTS	Proprietary S/w	Yes	Yes	No
Open RAN	COTS	Proprietary or Open S/w	No	Yes	Yes

TABLE 2. O-RAN working groups and their main focus.

Working Group	Focus/Goal
WG1	Overall Architecture and Use Cases
WG2	Non-real-time RIC and A1 Interface
WG3	Near-real-time RIC and E2 Interface
WG4	Open FH interfaces
WG5	Open F1/W1/E1/X2/Xn Interface
WG6	Cloudification and Orchestration
WG7	White Box Hardware
WG8	Stack Reference Design
WG9	Open X-haul Transport
WG10	OAM and its interfaces
WG11	O-RAN Security

approach with a collaborative methodology that is focused on building and deploying global telecom network infrastructure. TIP is more focused on deployments and execution of Open RAN than designing its specifications. It promotes plugfests and live deployments in the field. It is also involved in training and the implementation of Open RAN solutions around the world.

To enhance their collaboration in the development of interoperable Open Radio Access Network solutions, the O-RAN Alliance and TIP have announced a liaison agreement [53]. This agreement will facilitate referencing, information exchange, and validation activities between the two organizations, thereby reinforcing their shared commitment to the Open RAN cause.

B. O-RAN KEY ARCHITECTURAL PRINCIPLES

Overall, the Key architectural principles of Open RAN can be identified as Virtualization, Disaggregation, Open Interfaces, and Intelligence, which are briefly discussed below.

Virtualization of the RAN refers to the concept of decoupling the hardware and software used to build the RAN. Virtualization makes it possible to run the RAN functionality as (open) software running on generic hardware platforms, rather than using proprietary hardware. One of the benefits of virtualization is that it allows companies to use best-of-breed and cost-efficient hardware. Secondly, it will enable companies to address changing network demands by scaling the resources elastically. Virtualization also holds the potential to simplify the orchestration of the RAN through layered abstraction, thereby contributing to a significant reduction in operational costs.

Disaggregation allows splitting the BS into several functional units. In the case of 5G networks, the BS can be split into three logical units, RU, DU and CU. The CU can be additionally separated into two logical nodes, with one handling the control plane (CU-CP) and the other managing the user plane (CU-UP). Such a logical separation facilitates the deployment of diverse functionalities across various network locations and hardware platforms.

Open Interfaces refer to the standardized interfaces between different components of a RAN, which allow for interoperability between equipment from different vendors. This enables the mixing and matching of RAN equipment from various vendors [54], thereby combining the most suitable equipment for a given deployment scenario, taking into account factors such as performance, required features, schedule, and costs.

The RAN Intelligent Controller (RIC) is a key element of the O-RAN architecture that provides a platform for optimization of the RAN elements and resources. The RIC comes in two forms: Non-Real-Time RIC (Non-RT RIC), designed for non-real-time control and optimization, and the Near-Real-Time RIC, tailored for near-real-time control and optimization. Both RICs provide a platform to host third-party applications that could be powered by Machine Learning (ML)/Artificial Intelligence (AI) to orchestrate the RAN for a given use case [55]. These apps serve as use-case tailored algorithms for performing tasks such as Radio Resource Management (RRM) and functionalities associated with Self-Organizing Network (SON). The infusion of the external controller in RAN can be considered to efficiently manage and orchestrate network services in an intelligent manner with reduced cost [10].

C. 5G RAN ARCHITECTURE

The O-RAN architecture designed by the O-RAN alliance is built on top of the NG-RAN architecture proposed by the 3rd Generation Partnership Project (3GPP). Therefore, we first discuss the NG-RAN architecture and then follow with the O-RAN architecture.

NG-RAN is the “new generation” RAN for 5G [50]. The NG-RAN configuration can support Non-Stand-Alone (NSA) and Stand-Alone (SA) modes. In NG-RAN with 5G SA, the 5G Next Generation Next Generation NodeB (gNB) connects directly to the 5G Core (5GC), as shown in Fig. 3. The gNB connects to the core network via the NG interface and to the other gNBs using the Xn interface The Uu interface exists between an UE and the gNB [56].

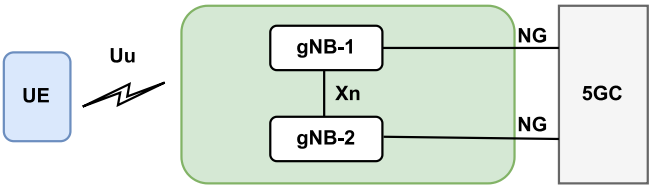

FIGURE 3. A basic 5G Stand-Alone network architecture.

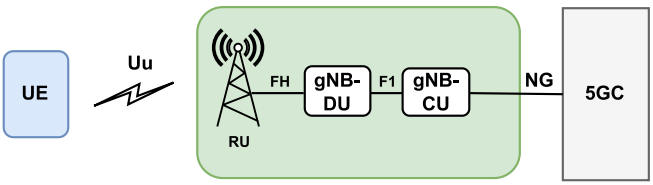

FIGURE 4. NG RAN split into gNB-DU and gNB-CU.

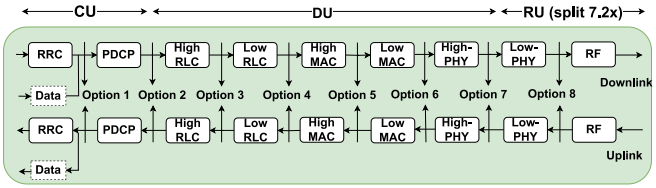

FIGURE 5. NG-RAN split options [59].

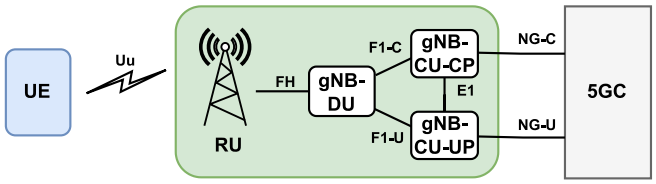

FIGURE 6. NG-RAN gNB-CU further split into gNB-CU-CP and gNB-CU-UP.

In NSA mode, both 4G and 5G base stations are used to exchange traffic with the UE and connect to the same core (Evolved Packet Core (EPC)). Note that the scope of this paper focuses on the adoption of 5G SA architectures within the O-RAN architecture.

In the 5G RAN architecture, the gNB can disaggregated into three main building blocks: RU, DU, and CU. Traditionally, the base station comprises of RU and BBU, but this division further separates BBU into DU and CU. This disaggregation divides base station functionality into three logical components, each hosting parts of the 5G protocol stack. Additionally, CU can be partitioned into CU-CP (Control Plane) and CU-UP (User Plane), further segmenting the 5G gNB protocol stack layers. The subsequent section provides a brief explanation of this 5G RAN split architecture.

CU-DU Split: The 3GPP specifications [17] supports the possibility of splitting a gNB (introduced in Fig. 3) into a gNB-Central Unit (gNB-CU) and gNB-Distributed Units (gNB-DUs) [50], often referred to as CU and DU, respectively. These logical nodes are connected via the F1 interface. The functional division between CU and DU is termed as the horizontal functional split [14]. Fig. 4, shows the NG-RAN architecture, with the CU-DU split visible for the gNB. Note that, regardless of whether a gNB is split into several units or not, it should always appear and behave to all other gNBs and the 5GC‘ as a single unit.

In order to distribute functionality between gNB-CU and gNB-DU, 3GPP evaluated several optional splits as shown in Fig. 5. Each of these functional splits offers a trade-off [57], [58]. They finally standardized the split option 2 for the general 5G architecture [50]. This split makes the gNB-CU host the Radio Resource Control (RRC), Service Data Adaptation Protocol layer (SDAP), and Packet Data Convergence Protocol (PDCP) layers, while the gNB-DU hosts the Radio Link Control (RLC), Media Access Control (MAC), and Physical layer (PHY) layers. This split between the DU and the CU brings better scalability according to User Plane traffic load.

CU-UP Split: The 3GPP specifications further allow the split of the gNB-CU (introduced in Fig. 4) into gNB-CU-Control Plane (gNB-CU-CP) and gNB-CU-User Plane (gNB-CU-UP), connected by the E1 logical interface, as shown in Fig. 6. The gNB-CU-CP hosts RRC and the control plane part of the PDCP protocol, while the gNB-CU-UP hosts the SDAP and the user plane part of the PDCP protocol. As shown in Fig. 6, gNB-CU-CP terminates the control plane part of the F1 interface towards the gNB-DU, while gNB-CU-UP terminates the user plane part of the F1 interface towards the gNB-DU. This further split allows the gNB to be composed of one gNB-CU-CP, one or more gNB-CU-UPs, and one or more gNB-DUs [50].

By adopting this split, mobile network operators gain the advantage of independently scaling the user plane without affecting the control plane, providing them with enhanced flexibility in network dimensioning [17]. Moreover, this segregation allows for customizable user plane configurations, catering to specific application requirements and reducing data transport delays to meet higher latency demands.

DU-RU Split: The 3GPP specifications have not standardized the RU functionality, i.e., they have not standardized a split between the DU and the RU, its implementation is left to the vendors. For instance, a split option supported by the O-RAN alliance is 7.2x, which involves using Split 7 between the RU and the DU, and Split 2 between the CU and the DU. Similarly, the Small Cell Forum supports split option 6 as the Lower Layer Split (LLS) Split.

V. O-RAN: ARCHITECTURE AND INTERFACES

The O-RAN architecture shown in Fig. 7 is based on the NG-RAN design put forth by the 3GPP, as already discussed.

Therefore, consistent with the NG-RAN architecture (discussed in Section IV-C), it also splits the RAN into RU, DU, and CU (CU-CP and CU-UP). In O-RAN language, these components are pre-fixed with O-, namely O-CU-UP,

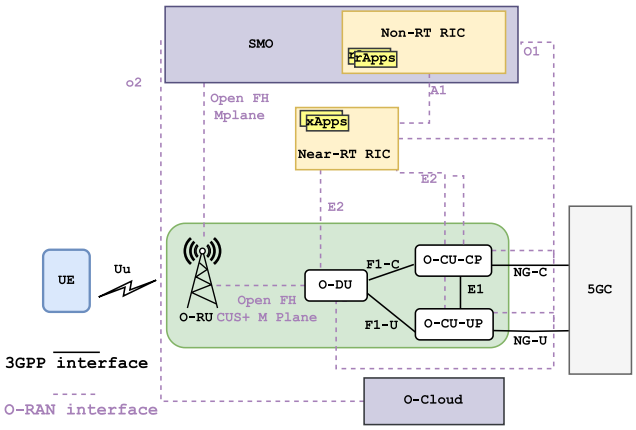

FIGURE 7. Logical O-RAN architecture [60]

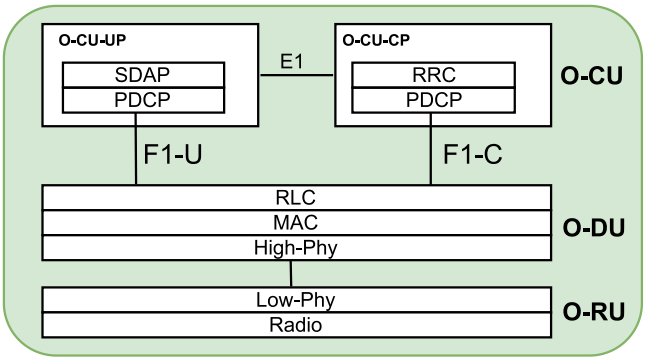

FIGURE 8. O-CU, O-DU, O-RU function split 7.2x.

O-CU-CP, O-DU, and O-RU, to refer to the fact that they are 3GPP-based functionalities adapted to O-RAN architecture.

Besides the functional split of a gNB, O-RAN introduces the concept of RAN Intelligent Controller (RIC), abstracting out RAN control and monitoring from a base station. It also defines Service Management and Orchestration (SMO) for network function management and O-Cloud (O-RAN Cloud) to host cloudified network functions. The architecture's components are interconnected through 3GPP interfaces as well as new open interfaces defined by the O-RAN alliance.

For their reference architecture, the O-RAN Alliance has chosen split option 7.2x. This architecture aligns with the 3GPP recommendation of implementing split option 2 for the high-level split (HLS) between the CU and DU. Furthermore, this decision incorporates split option 7 for the lower layer split (LLS) between the RU and DU. Fig. 8 shows the division of the NR protocol stack layers using the 7.2x split.

The main elements in the O-RAN architecture shown in Figure 7 are briefly described below.

A. O-RU

O-RU is the radio unit of the O-RAN architecture (physical node) [17]. The O-RU is connected to the O-DU using the Open FH interface. According to the split 7.2x, it hosts the Low-Phy layer and RF processing layers of the gNB protocol stack.

Based on the location of the precoding function O-RUs are classified into two types: Category A and Category B [61]. Category A O-RUs don't perform precoding rather it is done on O-DU, while Category B O-RUs execute the precoding operation themselves.

B. O-DU

O-DU is a logical node that hosts the RLC, MAC and High-Phy layer according to the 7.2x functional split option. The operations of the O-DU are controlled by O-CU. Data segmentation/integration, scheduling, multiplexing/demultiplexing, and other baseband processing tasks are performed in the O-DU.

C. O-CU

O-CU is a logical node that hosts RRC, PDCP, and SDAP protocols and provides layer 3 functions such as connection and mobility management. It is divided into O-CU-UP for user plane processing and O-CU-CP for control plane processing. Within this structure, O-CU-CP handles the RRC and control plane part of the PDCP protocols, while the O-CU-UP handles the user plane segment of PDCP and SDAP.

Additionally, the O-DU establishes connections with O-CU-CP and O-CU-UP through F1-C and F1-U interfaces, respectively. O-CU-CP connects to the Access and Mobility Management Function (AMF) in the 5GC, while O-CU-UP establishes a connection with the User Plane Function (UPF).

D. O-CLOUD

The O-Cloud is a cloud computing platform that consists of a number of physical infrastructure nodes that meet the O-RAN requirements to host the O-RAN functions such as Near-RT RIC, O-CU-CP, O-CU-UP, and O-DU [62]. It also houses their supporting software elements (e.g., Operating System, Virtual Machines, Container Runtime, etc.), and the corresponding management and orchestration functions.

The hardware infrastructure of the O-Cloud platform includes compute, networking, and storage components, potentially incorporating acceleration technologies essential for RAN network functions to meet performance objectives [63]. Moreover, the O-Cloud platform software exposes open and well-defined Application Programming Interfaces (APIs), facilitating the seamless orchestration and management of both the Network Function deployment life cycle as well as the broader O-Cloud infrastructure.

E. SMO

In a Service Provider's Network, various domains such as RAN, Core, Transport, and Slice Management coexist [62]. Among the various domains SMO specifically manages the RAN domain [64] in the O-RAN architecture. SMO basically serves as the Orchestration and Management framework in O-RAN architecture [14]. The SMO framework encompasses

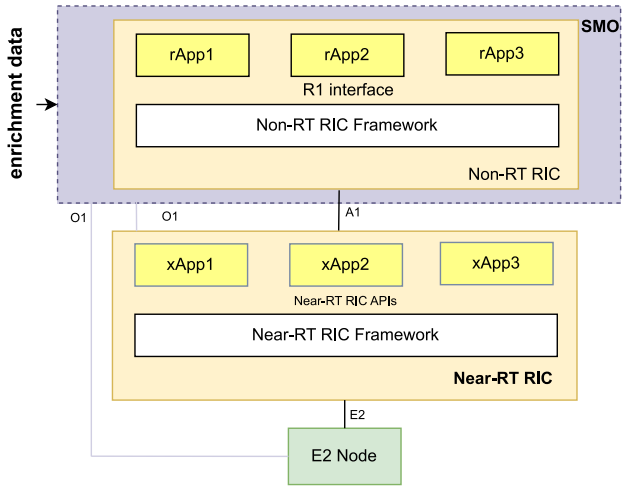

FIGURE 9. Near-RT RIC and Non-RT RIC.

several components and interfaces, including, O1, O2, Open FH M-Plane, A1, and Non-RT RIC.

The O1, O2, and O-FH M-Plane serve as management interfaces (including Fault, Configuration, Accounting, Performance, Security (FCAPS)) [65] in the O-RAN architecture and are controlled by the SMO. The SMO uses the O1 interface to manage all RAN elements but the O-RU. It uses the O2 interface to manage O-Cloud platform resources and workload (e.g., scaling up/down resources). O-FH M-Plane acts as a management interface for the O-RU. The Non-RT RIC (described below) interacts with the Near-RT-RIC via the A1-interface, e.g., for RRM.

F. RAN INTELLIGENT CONTROLLER (RIC)

The RIC in the O-RAN architecture provides an environment for programmable components capable of running optimization routines to monitor and control the RAN. The RIC serves as the host for functionalities traditionally found at the base station (Evolved NodeB (eNB) or gNB), including mobility management, admission control, and interference management [65]. These functionalities are accessible as applications on the controller within the RIC. The decisions made by these applications are subsequently enforced through open interfaces. These applications shall operate based on network state, traffic conditions, and goals of the Mobile Network Operator (MNO) and could be implemented using AI/ML algorithms.

The O-RAN architecture includes two types of RICs: Non-real-time (Non-RT) RIC and Near-real-time (Near-RT) RIC, depicted in Fig. 9.

The *Non-RT RIC* is a logical function of the SMO that supports control and optimization of RAN resources and elements on a non-real time basis. Its primary purpose is to provide policy-based guidance, enrichment information, and management of the ML models to complement the Near-RT RIC in optimizing the RAN [62].

The Non-RT RIC is designed for control loops with durations exceeding one second, focusing on establishing policies for higher network layers. This enables the deduction of trends in the network over various time intervals (e.g., hour, week), optimizing the overall RAN behavior.

The Non-RT RIC consists of Non-RT RIC Applications (rApps) and the Non-RT RIC Framework. The Non-RT RIC Framework is responsible for logically terminating the A1 interface and exposing a set of R1 services to rApps via the R1 interface (defined in next section) [66].

rApps are modular third-party applications tailored for the Non-RT RIC, delivering value-added services by leveraging the functionalities available in the SMO/Non-RT RIC Framework. The rApps communicate with the Non-RT RIC platform via the open R1 interface. Operating on the management plane, rApps contribute to providing value-added services related to RAN operation and optimization. The rApps encompass a wide array of functionalities, spanning radio resource management, data analytics, delivery of enriching information, provisioning of policy-based guidance, and AI/ML training. These rApps are designed to run on any vendor's Non-RT RIC because they are based on the open interface [67]. Additionally, rApps can be independently developed by different companies than the SMO/Non-RT RIC platform vendors and can receive upgrades separately from the SMO platform. Some examples of rApps are energy saving management, QoE prediction and assurance, coverage, and capacity management [65].

The *Near-RT RIC* is a software platform that enables xApps to control the RAN [68], [69]. This platform allows near real-time control of E2 nodes via actions sent over the E2 interface. The term E2 nodes refer to all units controlled by the Near-RT RIC such as O-DU, O-CU-CP, and O-CU-UP. The control of E2 nodes via xApps is supported by the Near-RT Framework that hosts a database storing network state and supports functionalities such as xApp management, conflict resolution as well as security. Additionally, it supports AI/ML workflows and offers APIs for xApp integration [68]. An overview of the Near-RT RIC is shown in Fig. 10.

The Near-RT RIC control is steered by the policies and assisted by models provided by the Non-RT RIC via the A1 interface. The Near-RT RIC operates within a near-real-time control loop, with a latency between ten milliseconds and one second. This time-frame corresponds to the execution of xApps, making decisions on control actions, generating policy updates, and collecting key performance measurements.

xApps are microservice-based applications tailored to operate on the Near-RT RIC. These applications are hosted in the RAN domain and could be provided by third-party software companies. The xApps are required to follow a specified open API definition to be able to communicate with other parts of the RIC [65]. Upon registration with the Near-RT RIC platform, the xApp informs the Near-RT RIC platform about the type of data it wants to consume and the

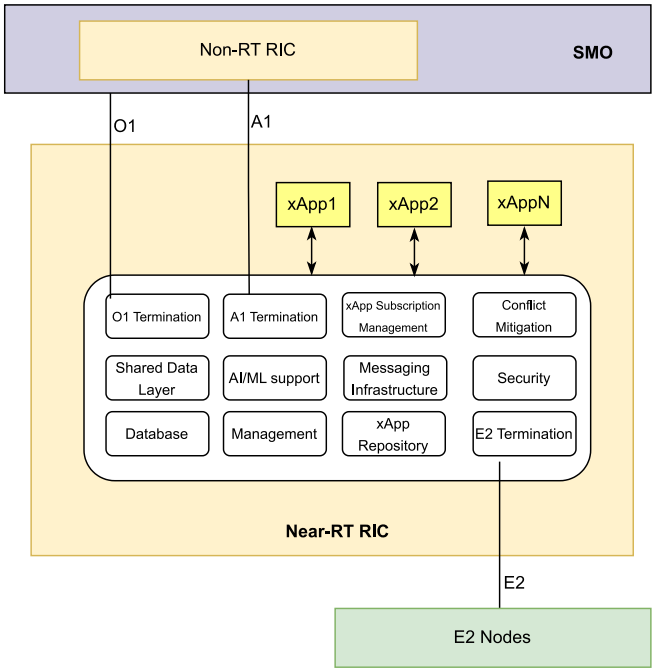

FIGURE 10. Near-RT RIC Architecture Overview.

outputs it will produce [55]. Some examples of xApp include mobility management, traffic steering, load balancing, and admission control.

VI. O-RAN INTERFACES FUNCTIONALITY AND SECURITY

In the following section, we briefly discuss the functionalities associated with the interfaces involved in the O-RAN architecture. Additionally, we discuss the required security measures. A comprehensive summary of the security requirements pertaining to each interface can be found in Table 3.

A. OPEN FRONTHAUL (FH) INTERFACE

The Open Fronthaul interface connects O-DU to O-RU [70], [71]. It divides the physical layer functionalities between O-RU and O-DU. The Open FH interface facilitates interoperability between various implementations of O-DU and O-RU.

The Open FH interface removes the traditional vendor-specific Common Public Radio Interface (CPRI) protocol and instead implements a newer and open eCPRI (enhanced CPRI) protocol. The information carried over the Open FH interface can be divided into four data planes: Control Plane (C-Plane), User Plane (U-Plane), Synchronization Plane (S-Plane), and Management Plane (M-Plane). The C-Plane carries real-time control information to the O-RU over eCPRI to define how U-Plane traffic should be handled. It should not be confused with UE's Control plane. The U-Plane refers to the real-time IQ sample data transferred between O-DU and O-RU. The S-Plane is used to achieve time, frequency, and phase synchronization between the clocks of O-DU and O-RU. The M-Plane [71] facilitates initialization, configuration, and management of the O-RU.

The existing specifications lack provisions for encryption and integrity protection of C-Plane, U-Plane, and S-Plane messages (also referred as CUS Plane). However, the U-plane is already protected using higher layer protection provided by PDCP [72] protocol. The PDCP protocol provides both confidentiality and integrity protection to the U-Plane data. Additionally, the specifications advocate for the use of IEEE 802.1X [73] to facilitate authentication and authorization in CUS planes. However, its implementation is mandatory in O-RU, while it remains optional in O-DU [61].

For the M-Plane, end-to-end security is mandatory. The security measures for the M-Plane include support for NETCONF/SSHv2 [74], [75] and NETCONF/TLS 1.2/1.3 [71].

B. A1 INTERFACE

In the O-RAN architecture, the A1 interface is an open logical interface between the Near-RT RIC and the Non-RT RIC [76]. This interface enables the Non-RT RIC to provide policy-based guidelines, manage the ML models (e.g., in xApps), and transfer enrichment information to the Near-RT RIC to facilitate the optimization of RAN functions. The data transferred over the A1 interface can be associated with a single UE or a group of UEs. Typically, a mechanism based on JSON is used to express information such as policies and intent. The A1 interface relies on the A1AP protocol, which combines REST APIs over HTTP for the transfer of JSON objects [15].

The *A1 policy management service* is used by the Non-RT RIC to guide the functionalities of Near-RT RIC towards the fulfillment of the goal expressed in *RAN intent* [76]. *RAN intent* refers to the expression of high-level operational or business objectives for a radio access network, enabling an operator to define the targeted Service Level Agreements (SLAs) that the RAN needs to fulfill for all or a class of users in a given area over a period of time. The policies are evaluated by the Non-RT RIC using the reporting functionalities of the O1 interface and the feedback received over the A1 interface. Based on the evaluation of the policies towards the fulfillment of RAN intent and some internal conditions, the Non-Real-RIC can then decide if it needs to issue/update the goals expressed in the A1 policies.

The *A1 enrichment information service* function enables the Near-RT RIC to improve the RAN optimization performance by providing information typically inaccessible to the RAN, such as data from non-network data sources. This information can be communicated to the xApps via A1EI or directly accessed by Near-RT from the Enrichment Information (EI) source. The Non-RT RIC will be responsible for the source authentication and security of the connection for the data provided by the external sources.

Regarding security, the A1 interface shall support confidentiality, integrity, and replay protection using TLS. It shall

TABLE 3. O-RAN interfaces security requirements. Light green cells represent mandatory security controls, gray cells represent optional security controls, and white cells represent no security control specified.

Security Control	A1	E2	O1	O2	R1	Open FH C-Plane	Open FH U-Plane	Open FH S-Plane	Open FH M-Plane
Confidentiality	TLS	IPSec	TLS	TLS	TLS	-	PDCP	-	TLS/SSH
Authenticity	TLS	IPSec	TLS	TLS	TLS	IEEE 802.1x	IEEE 802.1x	IEEE 802.1x	TLS/SSH
Integrity	TLS	IPSec	TLS	TLS	TLS	-	PDCP	-	TLS/SSH
Authorization	OAuth	-	NACM	OAuth	OAuth	IEEE 802.1x	IEEE 802.1x	IEEE 802.1x	NACM
Data Origination	TLS	IPSec	TLS	TLS	TLS	-	-	-	TLS/SSH
Reply Protection	TLS	IPSec	TLS	TLS	TLS	-	PDCP	-	TLS/SSH

also support mTLS for mutual authentication between the Non-RT RIC and one or more Near-RT RICs and use OAuth 2.0 [77] to support authorization [78].

C. E2 INTERFACE

The E2 interface is an open interface between the Near-RT RIC and the E2 nodes [79]. The E2 nodes maintain a one-to-one relationship with the Near-RT-RIC, while the Near-RT-RIC has a one-to-many relationship with the E2 nodes. The E2 interface allows the RIC to control functionalities and procedures related to E2 nodes. It also enables xApps to periodically gather data and metrics from the RAN or in response to specific trigger events. These data collection and control processes can pertain to single or multiple cells, slices, QoS classes, or UEs. The O-RAN alliance uses a variety of identifiers to support these operations, e.g., the UE ID for a specific UE. An E2 node can expose a variety of RAN functions based on the available adjustable parameters. These supported RAN functions can then be published by the E2 Node, and the xApps can subscribe to some of these functions.

The E2 interface has been logically divided into two protocols: E2 Application Protocol (AP) and E2 Service Model (SM). The E2AP protocol acts as a basic procedural protocol that [79] coordinates how E2 nodes communicate with the Near-RT-RIC.

An E2AP message can encapsulate different types of E2SMs, that implement specific functionalities [80]. Examples of these service models developed by O-RAN include, Key Performance Measurement (KPM) [81], RAN Control (RC) [82], and Cell Configuration and Control (CCC) [83].

Regarding security, the O-RAN security requirements [78] specifies that traffic on the E2 interface shall be protected using the IPsec [84] protocol. The IPsec protocol provides confidentiality, integrity, data origin authentication, and anti-reply protection.

D. O1 INTERFACE

The O1 Interface is an open interface between SMO framework and O-RAN managed elements (RAN nodes and near-RT RIC). Its main purpose is to facilitate the operation and management of O-RAN components, covering aspects such as FCAPS management, software management, and file management [17]. Essentially, the O1 interface enables the orchestration and management of all relevant O-RAN components and their associated network functions.

The O1 interface supports a range of Management Services (MnS) [85], including Provisioning, Fault Supervision, Performance Assurance, Trace Management, File Management, Software Management, Communication Surveillance, and more. It commonly links a MnS provider (usually the node managed by the SMO) to a MnS consumer (i.e., the SMO).

Regarding security [78], the O1 interface will enforce confidentiality, integrity, and authenticity using TLS 1.2 or higher. Additionally, it uses NACM [86] to enforce least privileged access.

E. O2 INTERFACE

In the O-RAN architecture, O2 is an open logical interface, that provides secure communication between SMO and the O-Cloud [87]. This interface enables the management of O-Cloud infrastructure and workload.

The services associated with the O-Cloud are categorized by O2 interfaces into two groups: Infrastructure Management Services (IMS) and Deployment Management Services (DMS). IMS encompasses a subset of O2 functions responsible for deploying and managing cloud infrastructure, including O-Cloud infrastructures, Scale-In and Scale-Out, FCAPS, and Platform Software Management. On the other hand, DMS includes a subset of O2 functions responsible for overseeing the life-cycle of virtualized/containerized deployments on the cloud infrastructure, such as Deployment, Termination, Scaling, and Healing of Network Function, along with their FCAPS.

Regarding security, the security specifications document [78] states that the O2 interface shall support confidentiality, integrity, replay protection, and data origin authentication. The interface would employ TLS to support these security requirements.

F. R1 INTERFACE

The R1 interface is an Open Interface between rApps and Non-RT RIC Framework that allows R1 Services to be produced and consumed [66]. The R1 services are typically available as APIs.

These APIs are being developed to help rApp developers implement RAN automation loops more quickly and easily by shielding low-level details. The R1 services includes [88], but not limited to, registration and discovery services, authentication and authorization services, AI/ML workflow services, and A1, O1, and O2 related services.

In terms of security, the R1 interface shall support TLS for protecting data at the transport layer, mTLS for mutual authentication between Non-RT RIC and rApps, and OAuth 2.0 for authorization [78].

VII. O-RAN USE CASES

The introduction of RICs, open interfaces, and AI/ML workflows enables the realization of advanced use cases and scenarios for RAN control and deployment optimization. The O-RAN Alliance has compiled an extensive catalog of 25 exemplary use cases for Open RAN deployment in [89], [90], with further high level details found in pertinent literature [22]. In this section, we provide a high level overview of a three important use cases defined by O-RAN Alliance, namely RAN Slicing, Context-Based Dynamic Handover and Energy Saving taken from the official O-RAN use case documentation. In particular, these use cases have been selected since they take advantage of the key features of O-RAN compared to monolithic solutions.

A. RAN SLICING

Network slicing in 5G leverages a single physical infrastructure to create multiple virtual networks, each tailored to specific requirements or tenants, enabling customized service provisioning. Performance requirements such as throughput, energy efficiency, latency, and reliability are detailed in Service Level Agreementss (SLAs) between operators and customers to ensure compliance and minimize violations [91]. Beyond the core network, the RAN must also be slice-aware, managing resource isolation, availability, and resource selection through RRM. O-RAN leverages open interfaces and ML platforms to support protective mechanisms and life cycle management for network slices within the RAN. Ensuring RAN slice service quality is challenging, but O-RAN's AI/ML architecture and open interfaces can enable effective SLA assurance, transforming network operations and business models [89].

The RAN slice SLA assurance use case involves interactions among the Non-RT RIC, Near-RT RIC, E2 nodes, and SMO. The use case starts with retrieval of RAN specific slice SLA/requirements (possibly within SMO). The Non-RT RIC performs long-term monitoring, trend analysis, and pattern recognition for RAN slice subnet performance. It also facilitates MLOps for tasks from data processing to model training and validation, enabling corrective actions like O1 reconfiguration or A1 policy creation. Moreover, the Non-RT RIC can deploy trained models to the Near-RT RIC for ML inference. The Near-RT RIC, in turn, executes AI/ML models in near-real-time, optimizing RAN operations based on O1 configurations, A1 policies, and slice-specific E2 measurements. The Near-RT also monitors slice specific RAN performance measurements [90].

B. THE CONTEXT-BASED DYNAMIC HANDOVER (HO) MANAGEMENT

The Context-Based Dynamic HO Management use case for Vehicle-to-everything (V2X) communication aims to optimize radio resource allocation, enhance road safety and reduce emission. V2X UEs, which are devices attached to vehicles, communicate with the V2X Application Server (V2X AS) to exchange critical information such as Cooperative Awareness Messages (CAMs) and radio measurements. As vehicles move, frequent and sometimes suboptimal handovers occur, leading to issues like short stays and ping-pong effects. To address these, this use case leverages AI/ML models deployed in the Near-RT RIC, based on data and policies from the Non-RT RIC, to customize handover sequences. Key entities involved include the Non-RT RIC for AI/ML model training and policy communication, the Near-RT RIC for model execution and policy enforcement, the RAN for configuration updates, and the V2X AS for data provision.

C. ENERGY SAVING (ES)

Energy Saving is a critical issue for network operators, especially with 5G networks. Due to varying traffic loads and user mobility, optimizing RAN Energy Consumption (EC) is complex and requires application across different network layers and timescales. The energy saving use case aims to leverage O-RAN AI/ML services and open interfaces to introduce optimized EC and energy efficiency (EE) solutions by switching network components on and off at various timescales. The ES use cases are divided into several sub-cases based on the control timescale and the system involved.

The first sub-case, Carrier and Cell Switch Off/On, operates on a non-real-time scale and involves turning off cells or carriers with no load or connected users, while neighboring cells manage the additional load. AI/ML-assisted solutions in the Non-RT RIC can be used to control the traffic load of the carriers and the cell, and to automatically decide when to switch off/on one or more carriers or a cell using O1 and/or Open fronthaul M-plane parameter configurations. Off/on switching is accompanied by adequate traffic steering, guided by policies, to ensure service continuity and Quality of Service (QoS).

The second sub-case, RF Channel Switch Off/On, aims to reduce power consumption of O-RU with massive MIMO deployment by switching certain RF channels on and off. This can operate at both non-real-time and near-real-time scales. AI/ML-assisted solutions via rApp or xApp can trigger this switching based on traffic information such as

load, user location, and mobility. For example, the algorithm can switch off 32 out of 64 RF channels in a digital M-MIMO architecture to save energy. The O-RU reconfiguration can be performed using the Open fronthaul M-plane from the E2 node or SMO. There is additional literature available on energy-saving strategies in O-RAN [35], [36], [37], [38].

VIII. O-RAN SECURITY LANDSCAPE

The O-RAN architecture introduces potential security risks beyond those in the 3GPP architecture [92]. These risks result from the inclusion of new functions, additional interfaces, and the Lower Layer Split. Additionally, the disaggregation of hardware and software, virtualization, increased automation, and the incorporation of open-source components introduces extra security challenges that need to be addressed.

To address such security risks, the O-RAN Alliance has established a dedicated working group, WG 11, that concentrates on the security aspects of the open RAN ecosystem [92]. This group is tasked with examining and defining threat models specific to O-RAN networks [92]. Additionally, WG 11 is responsible for specifying security requirements for each O-RAN interface and component [78], establishing implementation requirements for security protocols used by O-RAN [93], and documenting security tests to validate O-RAN implementations of security functions, configurations, and protocol requirements [94]. The overarching goal is to implement a robust zero-trust model.

A. THREATS AGAINST O-RAN

Threats related to O-RAN architecture can be broadly classified into seven categories which are briefly described below. The threat categories are taken from the O-RAN official O-RAN threat modeling documentation [92].

Threats against O-RAN elements

This category includes threats related to the components and interfaces standardized by the O-RAN alliance. The elements included in this category are: Open FH interface, A1 interface, R1 interface, O1 interface, SMO, O-RU, and RIC. These components may be subject to various types of attacks which could compromise the availability, integrity, and confidentiality of the network [92].

For example, the O-FH interface is vulnerable to Layer 2 threats [95]. An attacker who gains access to this interface can eavesdrop on all traffic. The lack of a security mechanism for this interface can allow an attacker to identify hosts, packet content, and traffic types. These actions could lead to the injection of a false message while impersonating a legitimate node, delay or reply of a legitimate message, or corrupting original messages, especially for the CUS plane [95]. Similarly, SMO also faces several potential threats. These include the importation of poisoned external data to influence decision-making processes, introducing corrupted data to execute remote code, exploiting weak authentication and authorization mechanisms, and targeting vulnerabilities in the APIs [96].

Threats against O-Cloud: The security threats that are pertinent to virtualization and containerization [97], [98], [99] are of significant concern to the O-Cloud. Common category of threats related to virtualization includes exploitation of Virtual Network Function (VNF), Container Network Function (CNF) images and their corresponding covert data; malicious usage of VM/CN to target other VM/CN, hypervisor/container engine.

O-Cloud's vulnerability extends to threats associated with the O2 interface, where an attacker on the SMO layer may exploit the O2 interface to gain unauthorized access to O-Cloud, and conversely, an attacker on O-Cloud may utilize the O2 interface to launch an attack on the SMO [92]. Additionally, API security threats are also shared by O-cloud or O-RAN in general.

Threats related to open-source code: The usage of open-source code in software development can be used as an attack vector to perform malicious activities [100], [101]. Potential attack vectors include, implanting intentional backdoors by malicious developers, spreading vulnerabilities through code reuse, leveraging publicly disclosed vulnerabilities, and human error [18]. Although O-RAN open-source components but is not strictly open-source.

Physical Threats: If a malicious actor gains physical access to the hardware, O-RAN components could be sabotaged, or sensitive data could be accessed. O-RAN's hardware can be rendered vulnerable due to issues such as improper security protection of data centers, insufficient protection against power outages, improper monitoring and maintenance of hardware parameters, and hardware backdoors [92].

Physical access to O-RAN components becomes a significant concern due to issues such as unsecured management ports and consoles, relaxed administrator credentials, and unsecured hardware/software configuration/management. Such issues can allow an adversary to inject malware, manipulate existing software, steal unprotected private keys and certificates, and turn off security features.

Threats against 5G radio networks: An adversary could use the readily available wireless channel to perform active and passive attacks. In active attacks [102], the adversary could actively transmit signals to influence what a UE or network would receive. Active attacks can be performed mainly using three techniques: Radio Jamming, Signal Overshadowing, and Message attacks [103]. In Radio Jamming, the adversary increases the noise on the wireless channel to perform attacks such as DoS or Downgrade a UE to a lower mobile network generation. Signal overshadowing is a new attack technique where an adversary overshadows a legitimate message without interfering with the synchronization between the BS and the victim UE. It can be used to perform attacks such as DoS, Signal Storming, Downgrade [104], [105]. In message attacks, the adversary uses fake devices such as a fake BS, MITM relay, or fake UE to perform the attacks. The attacks in this category span from

downgrading to lower generations (e.g., 4G or 2G) [106], DoS attacks [107], sending fake emergency messages [108], location spoofing [107], DNS spoofing [109], and more. Passive attacks usually involve a passive sniffer and can used to fingerprint devices [110], [111] or to decrypt phone calls [112].

Threats related to ML/AI: The application of AI/ML for O-RAN control can expose it to AI/ML-related attacks [113]. Possible threat categories against AI/ML are Model Alteration, ML Model Corruption, Evasion, Membership Inference, Data Property Inference, Data Reconstruction (theft), Model Extraction or Resource Exhaustion. [114], [115], [116].

Threats to Protocol Stack: The O-RAN alliance reveals the underlying protocol stack utilized within the O-RAN architecture. While this transparency is beneficial, it also creates opportunities for potential attacks across its layers due to factors such as improper implementation, utilization of weak ciphers, and zero-day exploits. These attacks may involve injection, cross-site scripting, denial of service, unauthorized exposure of object identifiers, and exploitation of Web tokens through REST APIs, JSON, or HTTP exploits [15].

B. COMPARISON OF TRADITIONAL RAN AND O-RAN THREAT SURFACE

Although the O-RAN architecture introduces new interfaces and components on top of the 3GPP RAN architecture and standardizes some existing elements, these additions do not fundamentally differentiate O-RAN from the more traditional 3GPP RAN regarding its internal operations. Some of the components and interfaces in the O-RAN are not entirely new to the RAN architecture; instead, they have been present in the RAN for a long time but were implemented in a vendor-specific manner (e.g., management and orchestration systems, front haul interface). Some of the components and interfaces were introduced in the RAN more recently due to the introduction of functional splits in the 3GPP RAN and the proliferation of Cloud RAN. While other components have been directly inherited from the 3GPP architecture.

Due to these similarities, the security risks associated with the O-RAN architecture closely align with those of the 3GPP RAN. These risks include design flaws, software security considerations, network security risks, and risks related to existing RAN components like O-RU, O-DU, or O-CU.

Among the elements present in the O-RAN (discussed in Section VI) only some of the elements are unique to O-RAN. According to a recent security report [20], a component or interface is not considered unique to O-RAN architecture, if its functionality already exists in more traditional (non-open) RANs, regardless of whether it has been newly specified by the O-RAN standards or not. Based on the above criteria, Non-RT RIC and Near-RT RIC, R1, E2, and A1 interfaces along with rApps, xApps, and their associated Machine Learning (ML) models, are considered unique to O-RAN. The report further states that the introduction of these new elements only contributes to 4 percent of the total threats against O-RAN discussed in the O-RAN threat modeling report [92]. While risks related to AI/ML have already been discussed in the section above, we briefly discuss the threats related to newly introduced elements in the next section.

C. THREATS UNIQUE TO OPEN RAN

As discussed above, unique to O-RAN are components such as Non-RT RIC, Near-RT RIC, interfaces R1, E2, and A1, along with the integration of AI/ML. The threats associated with these components are briefly discussed below.

1) THREATS RELATED TO NEAR-RT RIC

The incorporation of Near-RT RIC, utilizing xApps to control the RAN in the O-RAN architecture, introduces potential threats outlined below.

Malicious xApps can be deployed on the Near-RT RIC due to missing security measures around the deployment of xApps on the Near-RT RIC [92]. The malicious xApps could exploit the weakness to gain unauthorized access to E2 nodes, misuse radio network information, and control capabilities over the RAN functions [117]. Consequently, it can adversely impact the services of a particular subscriber or a dedicated area. These malicious xApps can also exploit UE identification, monitor UE location, and alter UE priority. For instance, if a malicious xApp receives an order via A1 policy to prioritize a specific UE, then the xApp owner knows an important person it wants to monitor in a particular area [97]. Based on this information, the adversary can track the rough location of the UE or alter the order from prioritize to de-prioritize. Note that the O-RAN specifications have proposed a Security function to prevent xApps from performing malicious activities.

Conflicting xApps The xApps in the Near-RT can be provided by different vendors and can make conflicting decisions if they are not coordinated properly [97]. These conflicts can be unintentional or malicious and could impact system functions such as mobility management, load-balancing, and admission control to degrade network availability or performance. For instance, xApps for Mobility Management and Load-balancing can issue different handover decisions for the same UE at the same instance, leading to the risk of triggering a radio link failure. Additionally, there is a possibility of xApp's decision conflicting with the internal decisions of the O-gNB. The O-RAN WG3 [68] lists three types of conflicts between xApps:

- *Direct conflict:* Change of the same parameter is requested by different xApps.
- *Indirect conflict:* Change of different parameters is requested by different xApps but creates opposite effects. E.g., antenna tilts and measurement offsets represent distinct control points, but both influence the handover boundary [97].
- *Implicit conflicts:* Change of different parameters is requested by different xApps that do not create obvious opposite effects but result in the degradation of the

overall network performance. Implicit conflicts are most difficult to mitigate since the correlations can hardly be observed.

These conflicts can lead to performance degradation and instabilities, potentially introducing vulnerabilities that threat actors could exploit to compromise system security

An optional Conflict Mitigation function (E2 Guidance Request Procedure) can mitigate conflicts arising from new xApps [68], [117]. It allows new xApps to obtain guidance from the Conflict Mitigation function to resolve potentially overlapping or conflicting requests from multiple xApps. It is possible to resolve direct conflicts using this procedure. However, since indirect and implicit conflicts cannot be observed directly, they may or may not be resolved, depending upon the relationship between the xApps [15].

2) THREATS RELATED TO NON-RT RIC

The introduction of Non-RT RIC in the O-RAN architecture brings about potential threats outlined below.

Threats against Non-RT RIC: Attackers can exploit SMO channels to launch DoS attacks, track UE, or degrade performance due to unspecified security measures [92]. This could hinder crucial functions like A1 policy analysis, updates, and secure data delivery to Near-RT RIC.

Conflicting rApps can disrupt O-RAN functions, leading to performance degradation or triggering a Denial of Service (DoS). The rApps in the Non-RT RIC can be provided by different suppliers that can introduce the potential for these applications to make conflicting decisions, leading to contradictory policies. These conflicts, encompassing direct, indirect, and implicit types, are challenging to mitigate due to unobservant dependencies [92].

Malicious rApps can be deployed and exploited by attackers. These rApps may originate from untrusted sources or seemingly trusted sources that intentionally insert backdoors into the applications. Exploitable rApps can enable an attacker to disrupt network services and potentially take over other rApps or the entire Non-RT RIC. The malicious rApps can impact Non-RT RIC functions such as AI/ML model training, A1 policy management, enrichment information control, and Network Configuration Optimization. The objective behind these malicious activities includes performance degradation, initiating DoS attacks, and gaining unauthorized access to data such as UE location and navigation details [92].

3) THREATS RELATED TO NEW INTERFACES

The introduction of new interfaces in the O-RAN architecture brings about potential threats outlined below:

Threats to E2 interface The E2 interface uses IPsec to protect the traffic on the interface [78]. Despite this security measure, there remains a potential vulnerability where end users may generate data that appears legitimate but is, in fact, malicious. This introduces a risk of potential attacks, particularly when the system lacks robust deep data inspection capabilities to identify malicious content. For example, ingeniously crafted data might give rise to attacks such as buffer-overflow or SQL injection [17]. Additionally, in the presence of weak mutual authentication, a malicious E2 node could exploit vulnerabilities to communicate with the Near-RT RIC, allowing for the monitoring or modification of messaging across the E2 interface [92].

Threats related to R1 interface The R1 interface employs TLS, mTLS, and OAuth to safeguard against potential threats [78]. However, the presence of weak mutual authentication can introduce vulnerabilities that may lead to a spectrum of potential threats. The threats include malicious actors gaining unauthorized access to R1 services, manipulating Service Heartbeat to cause DoS, bypassing authorization to discover sensitive data, and comprising data delivery to consumers, possibly leading to erroneous decisions [92].

Threats related to A1 interface TLS and OAuth contribute robust security to this interface [78]. However, the presence of weak mutual authentication poses a risk, potentially enabling a malicious Non-RT RIC to connect with Near-RT, allowing for unauthorized monitoring or manipulation of messages across the A1 interface [92]. Additionally, there is also a possibility of intelligent availability attacks on the A1 interface that can reduce the quality of service offered by the RAN [17].

IX. SUMMARY

Open RAN represents an innovative technology poised to disrupt the cellular industry ecosystem by addressing current challenges. Open RAN deployments are characterized by disaggregated, virtualized, software-based elements connected via open standardized interfaces, and can be managed using third-party applications. This approach promises to foster a multi-vendor ecosystem, enhanced flexibility, improved cost efficiency, and increased performance.

This paper provided a concise overview of Open RAN and its associated security considerations. Initially, we traced the evolution of RAN from traditional to virtualized forms to highlight the differences and advancements in RAN technology. Subsequently, we delved into the Open RAN movement, outlining its key architectural principles and the primary groups involved.

Furthermore, we elaborated on the interfaces within the architecture and the implemented security features. The security landscape section provides insights into various threat categories associated with Open RAN. A comparative analysis with traditional RAN architecture identifies unique elements introduced by Open RAN, such as Non-RT RIC, Near-RT RIC, R1, E2, A1 interfaces, as well as rApps, xApps, and their associated Machine Learning (ML) models. The paper then delves into specific threats related to these novel elements in the RAN, offering a comprehensive examination of the additional potential security challenges introduced.

REFERENCES

[1] S. D'Oro, L. Bonati, F. Restuccia, and T. Melodia, "Coordinated 5G network slicing: How constructive interference can boost network throughput," *IEEE/ACM Trans. Netw.*, vol. 29, no. 4, pp. 1881–1894, Aug. 2021.

[2] S. D'Oro, F. Restuccia, and T. Melodia, "Toward operator-to-waveform 5G radio access network slicing," *IEEE Commun. Mag.*, vol. 58, no. 4, pp. 18–23, Apr. 2020.

[3] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.

[4] X. Lin, "Artificial intelligence in 3GPP 5G-advanced: A survey," presented at Global Commun., 2024.

[5] Y. Azimi, S. Yousefi, H. Kalbkhani, and T. Kunz, "Applications of machine learning in resource management for RAN-slicing in 5G and beyond networks: A survey," *IEEE Access*, vol. 10, pp. 106581–106612, 2022.

[6] T. O'Shea and J. Hoydis, "An introduction to deep learning for the physical layer," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 4, pp. 563–575, Dec. 2017.

[7] *O-RAN: Towards an Open and Smart RAN*, O-Ran Alliance, Bonn, Germany, Oct. 2018.

[8] V.-G. Nguyen, A. Brunstrom, K.-J. Grinnemo, and J. Taheri, "SDN/NFV-based mobile packet core network architectures: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1567–1602, 3rd Quart., 2017.

[9] "Network functions virtualization—Network operator perspectives on NFV priorities for 5G," ETSI, Sophia Antipolis, France, White Paper, Feb. 2017.

[10] P. K. Thiruvasagam et al., "Open RAN: Evolution of architecture, deployment aspects, and future directions," Jan. 2023, *arXiv:2301.06713*.

[11] "'Open' telecom networks (open RAN): Towards the reconfiguration of international relations," IFRI, 2022. [Online]. Available: https://www.ifri.org/en/publications/notes-de-lifri/open-telecom-networks-open-ran-towards-reconfiguration-international

[12] F. Klement et al., "Open or not open: Are conventional radio access networks more secure and trustworthy than open-RAN?" 2022, *arXiv:2204.12227*.

[13] "Current state of open RAN." TeckNexus. 2022. Accessed: Mar. 3, 2023. [Online]. Available: https://tecknexus.com/5g-network/current-state-of-open-ran-countries-operators-deploying-trialing-open-ran/

[14] W. Azariah, F. A. Bimo, C.-W. Lin, R.-G. Cheng, N. Nikaein, and R. Jana, "A survey on open radio access networks: Challenges, research directions, and open source approaches," *Sensors*, vol. 24, no. 3, p. 1038, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/3/1038

[15] 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.

[16] 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.

[17] *Open RAN Risk Analysis*, Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany, 2022.

[18] *Open Radio Access Network Security Considerations*, Nat. Security Agency (NSA) Cybersecurity Infrastruct. Security Agency (CISA), Washington, DC, USA, Sep. 2022.

[19] *Report on the Cybersecurity of Open RAN*, NIS Group, North Liberty, IA, USA, 2022.

[20] *Open RAN Security Report*, Quad Crit. Emerg. Technol. Working Group, Nat. Telecommun. Inf. Admin., Washington, DC, USA, May 2023.

[21] 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. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804523000401

[22] 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./Dec. 2022. [Online]. Available: http://dx.doi.org/10.1109/MNET.108.2100659

[23] P. S. Upadhyaya, A. S. Abdalla, V. Marojevic, J. H. Reed, and V. K. Shah, "Prototyping next-generation O-RAN research testbeds with SDRs," 2022, *arXiv:2205.13178*.

[24] L. Bonati, M. Polese, S. D'Oro, S. Basagni, and T. Melodia, "OpenRAN gym: An open toolbox for data collection and experimentation with AI in O-RAN," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2022, pp. 518–523. [Online]. Available: http://dx.doi.org/10.1109/WCNC51071.2022.9771908

[25] M. Dryjański, Ł. Kułacz, and A. Kliks, "Toward modular and flexible open ran implementations in 6G networks: Traffic steering use case and O-RAN xApps," *Sensors*, vol. 21, no. 24, p. 8173, 2021.

[26] E. Coronado, S. Siddiqui, and R. Riggio, "Roadrunner: O-RAN-based cell selection in beyond 5G networks," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp.*, 2022, pp. 1–7.

[27] B. H. Prananto, Iskandar, and A. Kurniawan, "O-RAN intelligent application for cellular mobility management," in *Proc. Int. Conf. ICT Smart Soc. (ICISS)*, Bandung, Indonesia, 2022, pp. 1–6, doi: 10.1109/ICISS55894.2022.9915221.

[28] D. Johnson, D. Maas, and J. Van Der Merwe, "NexRAN: Closed-loop RAN slicing in POWDER-a top-to-bottom open-source open-RAN use case," in *Proc. 15th ACM Workshop Wireless Netw. Testbeds, Exp. Eval. Characterization*, 2022, pp. 17–23.

[29] R. Smith, C. Freeberg, T. Machacek, and V. Ramaswamy, "An O-RAN approach to spectrum sharing between commercial 5G and government satellite systems," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, 2021, pp. 739–744.

[30] M. W. Akhtar, A. Mahmood, S. F. Abedin, S. A. Hassan, and M. Gidlund, "Exploiting NOMA for radio resource efficient traffic steering use-case in O-RAN," in *Proc. IEEE Global Commun. Conf.*, 2022, pp. 5771–5776.

[31] A. Samorzewski, A. Kliks, and M. Dryjański, "QoS-based RRM procedure for O-RAN systems," in *Proc. 29th Annu. Int. Conf. Mobile Comput. Netw.*, 2023, pp. 1–3.

[32] L. Baldesi, F. Restuccia, and T. Melodia, "ChARM: NextG spectrum sharing through data-driven real-time O-RAN dynamic control," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, 2022, pp. 240–249.

[33] P. Sroka, U. Kulacz, S. Janji, M. Dryjański, and A. Kliks, "Policy-based traffic steering and load balancing in O-RAN-based vehicle-to-network communications," *IEEE Trans. Veh. Technol.*, early access, May 13, 2024, doi: 10.1109/TVT.2024.3399924.

[34] M. M. Qazzaz, Ł. Kułacz, A. Kliks, S. A. Zaidi, M. Dryjanski, and D. McLernon, "Machine learning-based xApp for dynamic resource allocation in O-RAN networks," 2024, *arXiv:2401.07643*.

[35] L. Wang, J. Zhou, M. Ma, and X. Niu, "Minimizing energy consumption of IoT devices for O-RAN based IoT systems," *Energy Rep.*, vol. 9, pp. 379–388, Nov. 2023.

[36] Ö. T. Demir, M. Masoudi, E. Björnson, and C. Cavdar, "Cell-free massive MIMO in O-RAN: Energy-aware joint orchestration of cloud, fronthaul, and radio resources," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 2, pp. 356–372, Feb. 2024.

[37] L. Wang, J. Zhou, Y. Wang, and B. Lei, "Energy conserved computation offloading for O-RAN based IoT systems," in *Proc. IEEE Int. Conf. Commun.*, 2022, pp. 4043–4048.

[38] M. Dryjański, *The O-RAN Whitepaper 2023—Energy Efficiency in O-RAN*, O-RAN Alliance, Alfter, Germany, 2023.

[39] "Accelerating 5G virtual RAN deployment," Comcores. 2020. [Online]. Available: https://www.comcores.com/wp-content/uploads/2020/07/O-RAN-Intro-whitepaper-1.pdf

[40] "5G open RAN ecosystem Whitepaper," NTT Docomo, Tokyo, Japan, White Paper, 2021. [Online]. Available: https://ssw.web.docomo.ne.jp/orec/5gopenranecosystem/whitepaper/OREC WP.pdf

[41] "Open RAN security white paper," Deutsche Telekom, Bonn, Germany, Orange, Paris, France, Telefonica, Madrid, Spain, Vodafone, Berkshire, U.K., White Paper, 2022. [Online]. Available: https://cdn.brandfolder.io/D8DI15S7/at/45zqtkzjp4n9ncn77mkqbx8/Open RAN MoU Security White Paper-FV.pdf

[42] M. Dryjanski and R. Lundberg, "The O-RAN Whitepaper 2021—Rimedo labs," 2021. [Online]. Available: https://www.rimedolabs.com/blog/the-o-ran-whitepaper/

[43] T. Nolle, "Transformation and 5G O-RAN—VMWare," 2021. [Online]. Available: https://telco.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/microsites/telco/vmware-transformation-and-5g-o-ran.pdf

[44] "Dell technologies, VMware, and Mavenir 5G O-RAN reference architecture," 2021. [Online]. Available: https://tinyurl.com/39bj9z4n

[45] "O-RAN: An open ecosystem to power 5G applications." VIAVI Solutiuons. 2021. [Online]. Available: https://www.viavisolutions.com/en-us/literature/o-ran-open-ecosystem-power-5g-applications-white-papers-books-en.pdf

[46] "OpenRAN RAN intelligence and automation," TIP, 2021. Accessed: Dec. 2022. [Online]. Available: https://cdn.brandfolder.io/D8DI15S7/at/xq2qrcwgszxpb49zt93bwt/RIA/OpenRANataglance_Glossy_v08_2021_06_16.pdf

[47] G. Brown, "TIP OpenRAN: Toward disaggregated mobile networking," 2020. [Online]. Available: https://cdn.brandfolder.io/D8DI15S7/as/qc19tk-54bsw-305

[48] "Security in open RAN." Altiostar, Jan. 2021. [Online]. Available: http://altiostar.com/wp-content/uploads/2021/02/Open-RAN-Security-White-Paper-January-2021.pdf

[49] S. P. J. S. Boswell, "Security considerations of open RAN," Ericsson, Stockholm, Sweden, White Paper, Aug. 2021. [Online]. Available: https://www.ericsson.com/4a67b7/assets/local/reports-papers/further-insights/doc/02092021-12911-security-considerations-for-cloud-ran.pdf

[50] X. Lin and N. Lee, Eds., *5G and Beyond: Fundamentals and Standards*, 1st ed. Cham, Switzerland: Springer Nat., 2021. [Online]. Available: https://doi.org/10.1007/978-3-030-58197-8

[51] "Everything you need to know about open RAN." ParallelWireless. 2020. [Online]. Available: https://www.parallelwireless.com/wp-content/uploads/Parallel-Wireless-e-Book-Everything-You-Need-to-Know-about-Open-RAN.pdf

[52] "xRAN forum merges with C-RAN alliance to form ORAN alliance." 2018. [Online]. Available: https://www.businesswire.com/news/home/20180227005673/en/

[53] A. Weissberger, "TIP OpenRAN and O-RAN alliance: Liaison and collaboration for open radio access networks," Feb. 2020. [Online]. Available: https://techblog.comsoc.org/2020/02/26/tip-openran-and-o-ran-alliance-liaison-and-collaboration-for-open-radio-access-networks/

[54] "O-RAN empowering vertical industry: Scenarios, solutions and best practice white paper," O-RAN Alliance e.V., Alfter, Germany, White Paper, Dec. 2023.

[55] "The O-RAN Whitepaper 2022—RAN intelligent controller," Rimedo Labs, Poznań, Poland, White Paper, Feb. 2022.

[56] "NG-RAN; architecture description," 3GPP, Sophia Antipolis, France, Rep. TS 38.401, Apr. 2022. [Online]. Available: http://www.3gpp.org/DynaReport/38401.htm

[57] "5G functional splits." Parallel Wireless. 2022. Accessed: Jan. 2, 2024. [Online]. Available: https://www.parallelwireless.com/wp-content/uploads/5G-Functional-Splits-V3.pdf

[58] D. Wypiór, M. Klinkowski, and I. Michalski, "Open RAN—Radio access network evolution, benefits and market trends," *Appl. Sci.*, vol. 12, no. 1, p. 408, 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/1/408

[59] "Technical specification group radio access network—Study on new radio access technology: Radio access architecture and interfaces (release 14), version 14.0.0," 3GPP, Sophia Antipolis, France, Rep. 38.801, Mar. 2017,

[60] "O-RAN Software Community: O-RAN architecture," Nov. 2022. Accessed: Apr. 17, 2023. [Online]. Available: https://docs.o-ran-sc.org/en/latest/architecture/architecture.html

[61] "O-RAN control, user and synchronization plane specification 13.0," WG4: Open Fronthaul Interfaces Workgroup, O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG4.CUS.0-R003-v13.00, 2023.

[62] "O-RAN architecture description 10.0," O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG1.OAD-R003-v10.00, Oct. 2023.

[63] "O-RAN cloud architecture and deployment scenarios for O-RAN virtualized RAN 5.0," WG6: Cloudification and Orchestration Workgroup, O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG6.CADS-v05.00, 2023.

[64] "O-RAN operations and maintenance architecture 10.0," O-RAN Alliance, Alfter, Germany, Rep. WG10: OAM for O-RAN, Rep. O-RAN.WG10.OAM-Architecture-R003-v10.00, 2023.

[65] A. Kliks, M. Dryjanski, V. Ov, L. Wong, and P. Harvey, "Towards autonomous open radio access networks," *ITU J. Future Evolv. Technol.*, vol. 4, pp. 251–268, May 2023.

[66] "O-RAN non-RT RIC architecture 4.0," O-RAN Working Group 2, O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG2.Non-RT-RIC-ARCH-R003-v04.00, Oct. 2023.

[67] "An intelligent platform: The use of O-RAN's SMO as the enabler for openness and innovation in the RAN domain," Ericsson, Stockholm, Sweden, White Paper BDGS-21:031169 Uen, Nov. 2021. [Online]. Available: https://www.ericsson.com/4aa80f/assets/local/reports-papers/white-papers/smo-enabling-intelligent-ran-operations.pdf

[68] "O-RAN near-RT RIC architecture 5.0," WG3: Near-real-time RIC and E2 Interface Workgroup, O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG3.RICARCH-R003-v05.00, 2023.

[69] M. Hoffmann et al., "Open RAN xApps design and evaluation: Lessons learnt and identified challenges," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 2, pp. 473–486, Feb. 2024.

[70] "O-RAN control, user and Synchronization plane specification 14.0: WG4: Open Fronthaul interfaces workgroup," O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG4.CUS.0-R003-v13.00, 2023.

[71] "O-RAN management plane specification 14.0: WG4: Open fronthaul interfaces workgroup," O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG4.MP.0-R003-v14.00, 2024.

[72] *NR; Packet Data Convergence Protocol (PDCP), Release 16, V16.6.0*, 3GPP Standard TS 38.323, Dec. 2021. [Online]. Available: https://www.3gpp.org/ftp/Specs/html-info/38323.htm

[73] *IEEE Standard for Local and Metropolitan Area Networks–Port-Based Network Access Control*, IEEE Standard 802.1X-2020, Feb. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9035631

[74] "Network configuration protocol (NETCONF)," IETF, RFC 6241, 2011. [Online]. Available: https://tools.ietf.org/html/rfc6241

[75] T. Ylonen and C. Lonvick, "The secure shell (SSH) authentication protocol," IETF, RFC 4252, Jan. 2006. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4252.html

[76] "O-RAN working group 2 (non-RT RIC and A1 interface WG) A1 interface: General aspects and principles," WG2: Non-real-time RAN intelligent controller and A1 interface workgroup, O-RAN Alliance, Alfter, Germany, Rep. o-RAN.WG2.A1GAP-R003-v03.01, 2023.

[77] D. Hardt, "The OAuth 2.0 authorization framework," IETF, RFC 6749, 2012. [Online]. Available: https://tools.ietf.org/html/rfc6749

[78] "O-RAN security protocols specifications 7.0," WG11: Security Work Group, O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG11.SecReqSpecs.0-R003-v07.00, Oct. 2023.

[79] "O-RAN E2 general aspects and principles (E2GAP) 4.01," WG3: Near-real-time RIC and E2 interface workgroup, O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG3.E2GAP-R003-v4.01, 2023.

[80] "O-RAN E2 service model (E2SM) 4.0," WG3: Near-real-time RIC and E2 interface workgroup3, O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG3.E2SM-R003-v04.00, Oct. 2023.

[81] WG3: Near-real-time RIC and E2 interface workgroup, "O-RAN E2 service model (E2SM) KPM 4.0," O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG3.E2SM-KPM-R003-v04.00, 2023,

[82] "O-RAN E2 service model (E2SM), RAN control 4.0," WG3: Near-real-time RIC and E2 Interface Workgroup, O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG3.E2SM-RC-R003-v04.00, 2023.

[83] "O-RAN E2 service model (E2SM) cell configuration and control 2.0," WG3: Near-real-time RIC and E2 Interface Workgroup, O-RAN Alliance, Rep. O-RAN.WG3.E2SM-CCC-R003-v02.00, 2023.

[84] K. Seo and S. Kent, "Security architecture for the internet protocol," RFC 4301, Dec. 2005. [Online]. Available: https://www.rfc-editor.org/info/rfc4301

[85] "O-RAN operations and maintenance interface specification 11.0," O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG10.O1-Interface.0-R003-v11.00, 2023.

[86] "Network configuration access control model," IETF, RFC 8341, 2018, [Online]. Available: https://tools.ietf.org/html/rfc8341

[87] "O-RAN O2 interface general aspects and principles 5.0," O-RAN Working Group 6, O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG6.O2-GA&P-R003-v05.00, 2023.

[88] "O-RAN R1 interface: General aspects and principles 7.0," O-RAN Working Group 2,O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG2.R1GAP-v06.00, 2023.

[89] "O-RAN use cases analysis report 13.0: WG1: Use cases and overall architecture workgroup," O-RAN Alliance, Rep. O-RAN.WG1.Use-Cases-Analysis-Report-R003-v13.00, Feb. 2024.

[90] "O-RAN use cases detailed specification 13.0: WG1: Use cases and overall architecture workgroup," O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG1.Use-Cases-Detailed-Specification-R003-v13.00, 2024.
[91] S. Marinova and A. Leon-Garcia, "Intelligent O-RAN beyond 5G: Architecture, use cases, challenges, and opportunities," *IEEE Access*, vol. 12, pp. 27088–27114, 2024.
[92] *O-RAN Security Threat Modeling and Remediation Analysis 6.0*, O-RAN Alliance, Alfter, Germany, Jun. 2023.
[93] "O-RAN security test specifications 5.0: WG11: Security work group,"O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG11.Security-Test-Specifications.O-R003-v05.00, 2023.
[94] "O-RAN security requirements and controls specification 7.0: WG11: Security work group," O-RAN Alliance, Alfter, Germany, Rep. O-RAN.WG11.Security-Requirements-Specification.O-R003-v07.00, 2023.
[95] D. Dik and M. S. Berger, "Open-RAN Fronthaul transport security architecture and implementation," *IEEE Access*, vol. 11, pp. 46185–46203, 2023.
[96] "Zero trust architecture for evolving radio access networks." Ericsson. Nov. 2023. [Online]. Available: https://www.ericsson.com/4ae256/assets/local/reports-papers/further-insights/doc/open-ran-security.pdf
[97] "Security considerations of open RAN." Ericsson. 2020. Accessed: Dec. 2023. [Online]. Available: https://www.ericsson.com/4ac698/assets/local/security/security-considerations-open-ran.pdf
[98] *Threat Analysis of Container-as-a-Service for Network Function Virtualization*, Fraunhofer Institute for Applied and Integrated Security (AISEC), München, Germany, 2024.
[99] M. Souppaya, J. Morello, and K. Scarfone, "Application container security guide," NIST, Gaithersburg, MD, USA, Rep. SP 800-190, 2024. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-190
[100] M. Ohm, H. Plate, A. Sykosch, and M. Meier, "Backstabber's knife collection: A review of open source software supply chain attacks," in *Detection of Intrusions Malware, Vulnerability Assessment*, C. Maurice, L. Bilge, G. Stringhini, and N. Neves, Eds. Cham, Switzerland: Springer 2020, pp. 23–43.
[101] P. Ladisa, H. Plate, M. Martinez, and O. Barais, "SoK: Taxonomy of attacks on open-source software supply chains," in *Proc. IEEE Symp. Security Privacy (SP)*, 2023, pp. 1509–1526.
[102] *Study on 5G Security Enhancement Against False Base Stations (FBS), Version 0.17.0, Release 17*, 3GPP Standard 36.331, 2021.
[103] M. S. Wani, M. Rademacher, T. Horstmann, and M. Kretschmer, "Security vulnerabilities in 5G non-stand-alone networks: A systematic analysis and attack taxonomy," *J. Cybersecurity Privacy*, vol. 4, no. 1, pp. 23–40, 2024. [Online]. Available: https://www.mdpi.com/2624-800X/4/1/2
[104] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, "Hiding in plain signal: Physical signal overshadowing attack on LTE," in *Proc. 28th USENIX Security Symp. (USENIX Security)*, Santa Clara, CA, USA, Aug. 2019, pp. 55–72. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/yang-hojoon
[105] S. Erni, M. Kotuliak, P. Leu, M. Roeschlin, and S. Capkun, "AdaptOver: Adaptive overshadowing attacks in cellular networks," in *Proc. 28th Annu. Int. Conf. Mobile Comput. And Netw.*, Oct. 2022, pp. 743–755. [Online]. Available: http://dx.doi.org/10.1145/3495243.3560525
[106] B. Karakoc, N. Fürste, D. Rupprecht, and K. Kohls, "Never let me down again: Bidding-down attacks and mitigations in 5G and 4G," in *Proc. 16th ACM Conf. Security Privacy Wireless Mobile Netw.*, 2023, pp. 97–108. [Online]. Available: https://doi.org/10.1145/3558482.3581774
[107] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "LTEInspector: A systematic approach for adversarial testing of 4G LTE," in *Netw. Distrib. System Security Symp.*, 2018, pp. 1–15. [Online]. Available: https://api.semanticscholar.org/CorpusID:3387805
[108] G. Lee et al., "This is your president speaking: Spoofing alerts in 4G LTE networks," in *Proc. 17th Annu. Int. Conf. Mobile Syst., Appl., Services*, 2019, pp. 404–416. [Online]. Available: https://doi.org/10.1145/3307334.3326082
[109] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, "Breaking LTE on layer two," in *Proc. IEEE Symp. Security Privacy (SP)*, May 2019, pp. 1121–1136.
[110] A. Shaik, R. Borgaonkar, S. Park, and J.-P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols: Exposing device capabilities," in *Proc. WiSec*, May 2019, pp. 221–231.
[111] M. Kotuliak, "LTE monitoring," M.S. thesis, ETH Zürich, Zürich, Switzerland, 2020.
[112] D. Rupprecht, K. S. Kohls, T. Holz, and C. Pöpper, "Call me maybe: Eavesdropping encrypted LTE calls with ReVoLTE," in *Proc. USENIX Security Symp.*, 2020, pp. 73–88. [Online]. Available: https://api.semanticscholar.org/CorpusID:219003307
[113] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," *Pattern Recognit.*, vol. 84, pp. 317–331, Dec. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0031320318302565
[114] "Adversarial machine learning: A taxonomy and terminology of attacks and mitigations," U.S. Dept. Commerce, NIST, Gaithersburg, MD, USA, Rep. NIST AI 100-2e2023, Mar. 2023, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.ipd.pdf
[115] N. N. Sapavath, B. Kim, K. Chowdhury, and V. K. Shah, "Experimental study of adversarial attacks on ML-based xApps in O-RAN," 2023, *arXiv:2309.03844*.
[116] E. Habler et al., "Adversarial machine learning threat analysis and Remediation in open radio access network (O-RAN)," 2023, *arXiv:2201.06093*.
[117] WG11: Security Work Group, "Study on security for near real time RIC and xApps," O-RAN Alliance, Rep. O-RAN.WG11.Security-Near-RT-RIC-xApps-TR.0-R003-v04.00, 2023.