Prudhvi Kumar Kakani[1], Hubert Djuitcheu[1], and Hans Dieter Schotten[1]

[1]Institute of Wireless Communication and Navigation, Rheinland-Pfälzische, Technische Universität Kaiserslautern-Landau (RPTU)

May 07, 2024

Evaluation of xApps and their Security in Next-Generation Open Radio Access Networks

Prudhvi Kumar Kakani*, Hubert Djuitcheu*, Hans D. Schotten*◇
*Institute of Wireless Communication and Navigation,
Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau (RPTU), Kaiserslautern, Germany.
{kakani, djuitcheu, schotten}@eit.uni-kl.de
◇Intelligent Networks, German Research Center for Artificial Intelligence (DFKI), Kaiserslautern, Germany.
Hans_Dieter.Schotten(at)dfki.de

***Abstract*—Within the context of the next-generation open radio access network (O-RAN), this paper provides a thorough analysis of xApps and their security. This research is anticipated to have a major impact on improving the security requirements and operational effectiveness of xApps. A wide range of subjects are covered in this paper, such as how xApps are built inside the O-RAN architecture, what security risks and vulnerabilities they provide, and how to reduce them. Through an examination of their architecture, vulnerabilities, and major security issues, it seeks to increase our understanding of xApps and make them more resilient. It addresses specific security issues including protecting the E2 interface and protecting against adversarial attacks and unwanted access to machine learning-based xApps. Additionally, the study explores the origins of vulnerabilities in xApps, such as compromised xApps, malicious xApps, and external agents. The mitigation strategies for xApps involve leveraging xApps to enhance O-RAN interface security, implementing centralized and distributed security measures, and adopting the xApp Repository Function (XRF) framework for authentication.**

***Index Terms*—xApps, Security, O-RAN**

I. Introduction

The evolution of telecommunications networks towards greater flexibility, scalability, and interoperability has led to the emergence of Next-Generation Open Radio Access Networks O-RAN. O-RAN represents a paradigm shift in the design and deployment of cellular networks, emphasizing disaggregation, open interfaces, and multi-vendor support to enable innovation and efficiency in network operations. Central to the O-RAN architecture are xApps, which are software applications that provide specific functionalities and services within the network environment.

As O-RAN deployments continue to expand and evolve, the evaluation of xApps and their security implications becomes paramount to ensure the integrity, reliability, and performance of network operations. The dynamic nature of xApps, coupled with the critical role they play in network management and optimization, necessitates a comprehensive assessment of their functionality, effectiveness, and security posture.

The paper delves into the radio access network (RAN) architecture, emphasizing the significant role of xApps in enabling non-real-time control of RAN elements and resources. It provides a categorization, and vulnerabilities of xApps, highlighting potential security threats such as Denial-of-Service (DoS) attacks, unauthorized access, Man-in-the-Middle (MitM) attacks, data privacy breaches, and adversarial attacks on machine learning (ML) based xApps. The study also explores the origins of vulnerabilities in xApps, discussing compromised xApps, malicious xApps, and external agents as potential sources of vulnerabilities.

Furthermore, the paper outlines risk mitigation strategies for xApps, including the use of xApps to secure new RAN interfaces, the implementation of centralized security xApps, distributed security to individual xApps, and the adoption of the xApp Repository Function XRF framework to ensure secure authentication and service discovery. It emphasizes the critical need for rigorous auditing, continuous monitoring, and adherence to best practices to overcome security challenges and strengthen the integrity of xApps in O-RAN networks.

The remainder of this paper is organized as follows: Section II offers a thorough review and analysis of the literature, as well as an architectural understanding of xApps, important components in O-RAN systems. Following this, Section III delves into the potential threats and vulnerabilities that xApps might encounter, thereby highlighting the security challenges they pose. In Section IV, we examine these security challenges and propose risk mitigation strategies to enhance the operation of Next-Generation O-RAN. The paper concludes in Section V, where we discuss possible future improvements to the security mechanisms for xApps.

II. xApp Background

A. Overview of O-RAN

The O-RAN architecture, illustrated in Figure 1, is structured around key components and open interfaces that break down base station functionalities into three main parts: the radio unit (RU), distributed unit (DU), and central unit (CU). The Open Radio Unit (O-RU) plays a vital role in handling radio frequency signals near the antenna, while the open Distributed Unit (O-DU) processes these signals before transmitting them to the network. Within the open Central Unit (O-CU) segment, the O-RAN Central Unit-Control Plane (O-CU-CP) manages control functions and protocols, while the O-RAN Central Unit-User Plane (O-CU-UP) focuses on user-centric operations and data transmission optimization. Intelligence in the O-RAN architecture is embodied by the Near-Real-time (RT)

RAN Intelligent Controller (RIC) and Non-RT RIC. The Near-RT RIC optimizes network components with rapid response times, hosting microservice-based xApps, to enhance spectrum efficiency. On the other hand, the Non-RT RIC orchestrates RAN functions intelligently in a non-real-time manner, supporting radio resource management, procedure optimization, and policy guidance. It centrally operates within the Service Management and Orchestration. (SMO) framework, enabling non-real-time control of RAN elements and resources through specialized applications called rApps. The Y1 interface plays a critical role in providing access to RAN analysis data for both internal and external processes. This interface is essential for sharing insightful information that can improve network performance and decision-making.

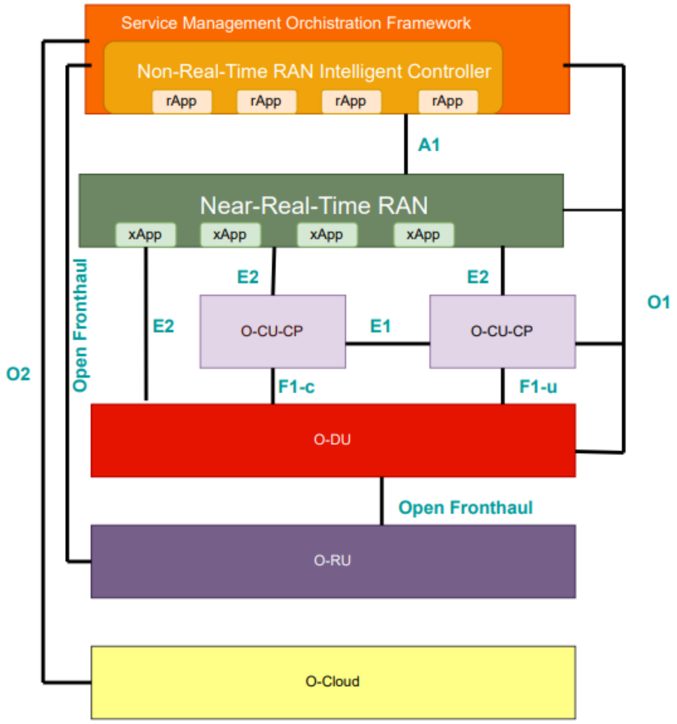

Fig. 1: O-RAN Architecture [1]

B. Literature Review

The concept of xApps within the O-RAN architecture, developed since the establishment of the O-RAN Alliance in 2018, addresses the need for programmability and flexibility in radio access network (RAN) environments. Evolving into integral components, xApps enable intelligent orchestration and dynamic decision-making in near real-time, promoting open and intelligent RAN solutions through ongoing collaboration and standardization efforts. As xApps become central elements of the O-RAN framework, they are ushering in a new era of flexibility and intelligence in RAN environments. This literature review examines existing research and advances in securing xApps to ensure their role in orchestrating and optimizing RAN functions is robust and reliable [1].

The deployment of xApps in the O-RAN architecture brings forth unique security challenges due to their modular and cloud-native architecture. Researchers emphasize the importance of robust security measures to address potential vulnerabilities and attacks, especially in the dynamic and distributed nature of xApp deployments. Authentication mechanisms are crucial for ensuring that only authorized xApps interact with the Near-RT RIC and other O-RAN components. Studies propose various authentication protocols tailored to xApp environments, focusing on secure identity verification. Data integrity and confidentiality in xApps, responsible for RAN function control, are safeguarded through encryption techniques and integrity verification mechanisms [2]. Security challenges associated with northbound and southbound interfaces are addressed with proposed secure communication protocols, access control mechanisms, and intrusion detection systems. The internal messaging framework within xApps, handling conflict mitigation and app lifecycle management, is secured through practices like secure coding, message encryption, and auditing mechanisms, enhancing overall xApp security [1].

C. xApps Architecture

The architecture of xApps within the O-RAN framework involves a modular and flexible design that allows these applications to run on the near-RT RIC as shown in the figure 2. xApp is an extended software application,is specifically designed to run on the RIC. This application, consisting of one or more microservices, clearly specifies the data it uses and provides at the onboarding stage. Importantly, xApp remains independent of the Near-RT RIC and can be supplied by third parties. The E2 interface provides a direct link between the xApp and the RAN functionality [3].

xApps are designed to actively control and enhance RAN functions. This encompasses tasks like dynamically modifying configurations, allocating resources, and adjusting other parameters to boost the overall efficiency of spectrum utilization, thereby contributing to enhanced network performance. xApps offers “northbound” interfaces, specifically A1 and O1, to the non-RT RIC. These interfaces enable communication and information exchange among different controllers, facilitating coordinated decisions and actions throughout the network. xApps gather data from various RAN functions, such as CUs and DUs, through the E2 interface. This interface acts as a communication conduit for data exchange, allowing xApps to receive real-time information from the RAN components. xApps incorporates an internal messaging framework to manage several critical functions. These include conflict mitigation to handle conflicting information or directives, subscription management to manage user preferences, and app lifecycle management to ensure efficient application operation. The security function is vital for network communication security, encryption, and authentication. By enforcing security rules, providing xApp schemes, and ensuring data integrity, the security function plays a pivotal role in preserving the security of the O-RAN system.

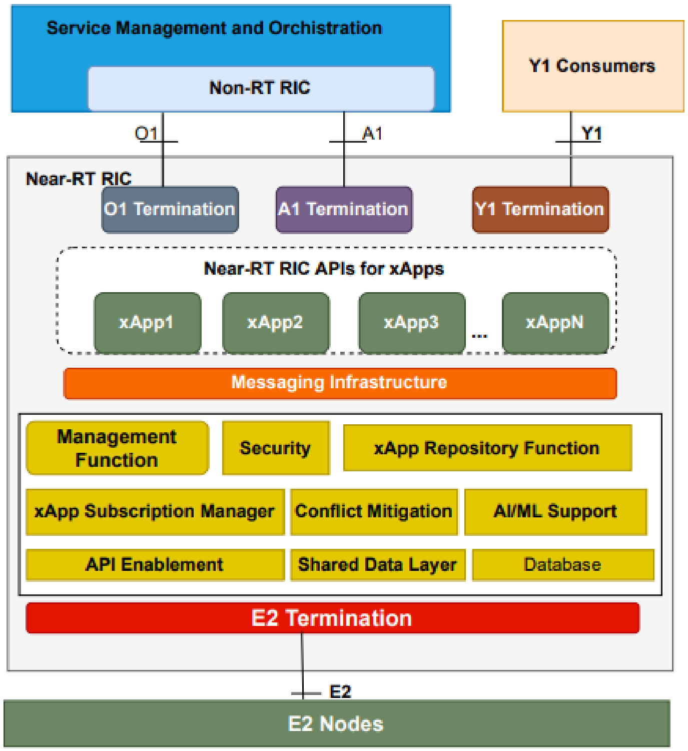

Fig. 2: Near RT Architecture with xApps [4]

D. Catagories of xApps

xApps are crucial in improving and managing various aspects of wireless communication networks. They provide a simple and effective way to manage radio resources, mobility, quality of service, and security. The ability of xApps to cross-connect is critical for ensuring seamless integration and interoperability across a wide range of technology domains. This establishes them as a critical component of wireless communication networks.

1) Radio Resource Management (RRM): The RRM category of xApps focuses on optimizing spectrum and radio resources. This includes dynamically allocating frequency bands, optimizing power levels, and managing interference to enhance overall network performance. xApps in this category dynamically allocate frequency bands based on current network demand, interference levels, and other factors. This ensures that each cell operates on a frequency that minimizes interference and maximizes throughput. xApps optimize the scheduling of transmissions within the network. This involves allocating time slots and spectrum resources to different users or devices, considering factors such as data priority, user requirements, and network conditions to improve overall spectral efficiency.

2) Mobility management: Mobility management xApps ensure seamless handovers as devices traverse the network. This includes overseeing the handover process between different cells or base stations, minimizing call drops, and maintaining uninterrupted connectivity for mobile users. These xApps monitor the movement of devices within the network, providing real-time location information. This data is vital for various location-based services and for optimizing network resources based on user density and movement patterns. The primary goal of Mobility Management xApps is to provide continuous connectivity for mobile devices. They facilitate smooth transitions between different radio access technologies, ensuring that users experience seamless connectivity, even during handovers.

3) quality of service (QoS): QoS based-xApps control and manage network traffic to maximize resource efficiency. They prioritize different types of traffic based on various criteria such as application requirements, user preferences, and service level agreements. These xApps detect network congestion and implement mitigation methods to prevent service degradation. Such strategies include changing resource allocation, redirecting traffic, and putting in place congestion avoidance devices. They also optimize latency, jitter, and packet loss to meet the requirements of real-time applications like voice calls and video streaming, thereby enhancing the overall quality of service across the network.

4) Security: Security-focused xApps manage user authentication, ensuring that only authorized devices and users have access to the network. Details the establishment of authentication mechanisms, which can range from simple username/password combinations to more advanced approaches like bio-metric verification. These security xApps additionally provide encryption techniques to protect communication channels within the RAN architecture. This measure is crucial to protecting sensitive information and preventing unauthorized access to or interception of data transmissions. Furthermore, security xApps enhance the overall security of the RAN architecture by deploying a variety of security measures. These include access control, intrusion detection, and response mechanisms. Together, these measures strengthen the network against potential security threats and vulnerabilities.

III. Vulnerabilities of xApps

This section discusses the vulnerabilities of xApps in the context of O-RAN. Initially, we examine the well-known and frequently encountered security issues related to xApps. Subsequently, we explore the recently introduced vulnerabilities, which are a result of the rapid evolution and rising complexity of xApps. Understanding these paradigms enables us to better anticipate potential security threats and design more resilient, secure systems for the future.

A. Common and New xApps Vulnerability Paradigms

Comprehending xApps vulnerabilities in O-RAN networks is essential to protecting against security threats and components that have been identified as potentially dangerous are covered below.

1) DoS: A Denial of Service attack presents a serious security risk to the O-RAN networks, particularly to the xApps in the Near-RT RIC. This type of attack can have a negative impact on the network ecosystem, starting with the xApps.

A DoS attack can interrupt xApps' services by overwhelming them with malicious traffic, resulting in service degradation or complete unavailability. In the O-RAN architecture, where xApps are critical for network performance orchestration and management, a DoS attack might disrupt network function orchestration and coordination, reducing overall efficiency. Furthermore, if the Near-RT RIC is subjected to a DoS assault, its real-time decision-making capabilities may be compromised, compromising the dynamic management and control of RAN resources. A DoS attack can cause service disruption, network instability, and degraded performance, emphasizing the critical need for strong security measures like traffic filtering, rate limiting, and proactive monitoring to protect xApps, O-RAN, and the Near-RT RIC from such malicious threats.

2) Unauthorized access: Unauthorized access to xApps poses a significant risk to network operations, user privacy, and the RIC. This can lead to data breaches, misuse of sensitive information, and manipulation of the RIC. Malicious actors can alter network behavior, causing service disruptions and degraded performance. They can also exploit sensitive user data, leading to privacy violations. Exploiting xApps vulnerabilities can cause system instability and disruptions, impacting network reliability [5]. Unauthorized control over network components, including the RIC, can lead to misconfigurations and unauthorized actions, affecting network integrity and security. Therefore, implementing robust security measures is crucial to prevent unauthorized access and protect the integrity of the RIC and the network.

3) MitM: In the context of O-RAN deployments, xApps are vulnerable to man-in-the-middle attacks. These attacks take place when malicious entities intercept and potentially modify the communication between xApps and other network components. The attacker positions oneself between the xApp and the intended communication endpoint, allowing them to eavesdrop on or modify the data exchange. This interception can compromise the confidentiality, integrity, and authenticity of the communication, providing a significant security risk to both the xApps and the broader network environment. MitM attacks on xApps can lead to unauthorized access to sensitive data, changes in network behavior, and even service interruptions. To prevent MitM attacks, it is critical to establish strong encryption, authentication systems, and secure communication protocols. These security measures protect xApps while also ensuring the security of the O-RAN ecosystem.

4) Privacy Violation: xApps are vulnerable to data privacy breaches owing to the sensitive nature of the data they handle and analyze. This data, which includes user information and network configurations, requires strict security measures to prevent unwanted access and disclosure. Without proper encryption and secure communication protocols, data exchanged between xApps and network components is vulnerable to interception or alteration. Furthermore, interactions with third-party services might raise the risk of data disclosure to unauthorized parties if access rules are not properly maintained. Inadequate data storage security measures might potentially leave stored data vulnerable to breaches, jeopardizing user privacy. To overcome these issues, firms must establish stringent security methods such as encryption, access limits, and compliance with data privacy laws.

5) Adversarial Attacks on ML-based xApps: These types of vulnerabilities pose a serious security risk by leveraging flaws in the ML models to manipulate their behavior and compromise the integrity of decision-making processes [6]. These attacks involve creating malicious inputs especially designed to deceive ML algorithms, leading to inaccurate predictions or decisions by the xApps. In O-RAN networks, adversarial attacks on ML-based xApps can have detrimental effects on network performance, security, and reliability. By introducing minor perturbations to input data, attackers might fool ML models into making incorrect conclusions, potentially resulting in network failures, service outages, or unauthorized access to vital resources. Adversarial attacks highlight the importance of implementing robust security measures such as adversarial training, input validation, anomaly detection, and model monitoring to detect and mitigate their impact. Furthermore, continuous evaluation and enhancement of ML models, as well as the incorporation of defense mechanisms against these threats, are essential to ensuring the resilience and effectiveness of ML-based xApps in O-RAN deployments.

B. Origins of vulnerabilities in xApps

In recent studies, authors in [7] have focused on investigating the primary sources and origins of attacks in O-RAN, with a particular emphasis on the Near-RT RIC and E2 interface. The following components present in the operation of the Near-RT RIC have been identified as potential sources of vulnerabilities.

1) Compromized xApps: These are xApps that have been infiltrated or exploited by malicious actors. Malicious actors may exploit compromised xApps to perform attacks such as data breaches, DoS, or unauthorized access to network resources. The compromised xApps may exhibit abnormal behavior, deviating from their intended functions and potentially causing disruptions or anomalies in network operations.

2) Malicious xApps: xApps that have been intentionally designed or manipulated to perform harmful actions, compromise network security, or disrupt normal operations. Malicious xApps can manifest in various forms, including malware-infected applications, rogue programs designed to steal data, or applications with backdoor access for unauthorized control. These xApps may attempt to bypass security controls, escalate privileges, or execute malicious commands within the network environment, compromising the overall security posture of the O-RAN networks.

3) External Agents: External vulnerability agents refer to terminators such as E2, A1, O1, and Y1 that connect the Near-RT RIC with other network components and can interact, either directly or indirectly, with the xApps. These exchanges can initiate malicious activities targeting the xApp. These agents represent a significant security concern as they can exploit vulnerabilities within the network infrastructure, leading to potential disruptions or compromises in the network's operation.

IV. xApps Risk Mitigation Strategies

This section explains the various considerations that xApps may use to solve security challenges, with an emphasis not only on interactions between xApps but also on interactions with other O-RAN open interfaces that connect with the near-RT RIC.

A. *xApps as security enabler for O-RAN*

xApps are engineered to augment network speed and enable encrypted communication across various interfaces. They utilize real-time data and analytics to effectively monitor network conditions for anomalies and security threats. Upon detecting irregular traffic patterns or data transmissions, xApps can initiate alerts and implement proactive security measures to mitigate potential risks. These applications play a crucial role in enforcing security policies and protocols by instituting access control mechanisms, encryption standards, and authentication procedures. This safeguards data transmission and prevents unauthorized access. For example, xApps ensure that only authenticated devices and users gain network access, thereby reducing the susceptibility to cyber-attacks. Furthermore, xApps facilitate dynamic resource allocation and management to optimize network performance while maintaining security standards. During periods of peak traffic or network congestion, xApps adeptly allocate resources to guarantee uninterrupted data transmission without compromising security, thus enhancing both the user experience and network protection. In essence, xApps are intelligent agents that improve the security of linked interfaces by analyzing data in real time, enforcing security regulations, and managing resources. Their proactive monitoring and management of network activity are critical for maintaining a secure and high-performance fifth generation (5G) environment. The combination of security xApps and machine learning algorithms improves security throughout the O-RAN network, particularly at the E2 interface. This is accomplished by proactively adopting security mechanisms like encryption and authentication, and examining traffic patterns for anomalies [7].

B. *Using xApps to secure xApps*

As shown in Figure 2, the Near-RT RIC has security features to prevent malicious xApps from accessing radio network data or obtaining unauthorized control over RAN functionalities. This security feature is meant to secure sensitive user data, prevent unauthorized access to vital components, and ensure the integrity of network operations. However, this functionality has several restrictions. For example, if xApps are not correctly designed or configured, they may become insecure, resulting in data breaches and system instability. Unauthorized access to essential components can potentially cause network disruptions. This emphasizes the need for strong authentication techniques and safe coding practices to properly mitigate these threats by using XRF framework and security xApp as shown in Figure 3.

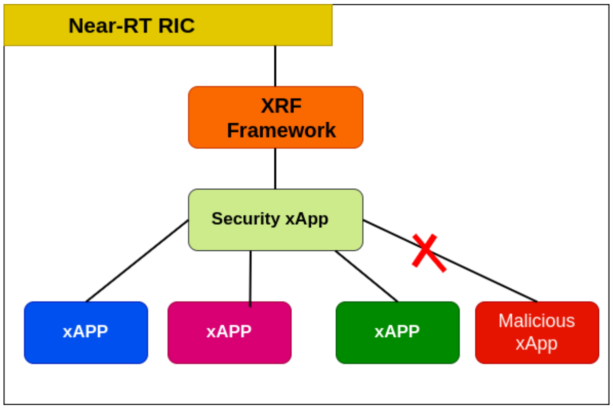

Fig. 3: Securing xApps by using XRF Framework and centralized Security xApp [2]

1) Centralized Security xApp: The concept of employing a dedicated security xApp to protect other xApps within the Near-RT RIC is not only feasible but also highly advantageous. This centralized security xApp plays crucial role in detecting and mitigating various types of attacks, such as DoS attacks, and tampering attacks across the network. By providing a unified platform for access control, encryption, and authentication methods, this security xApp streamlines security processes and enforces consistent security standards, thereby simplifying overall security management within the ecosystem [2]. Moreover, the centralized security xApp is capable of promptly identifying anomalies and potential security threats through real-time monitoring and analysis of network activities. This proactive approach enables the timely detection and mitigation of threats, bolstering the system's resilience against cyberattacks [8]. A key aspect of enhancing the functionality of this security xApp is the integration of machine learning capabilities. Leveraging machine learning algorithms, the xApp can analyze vast amounts of data to identify patterns, detect anomalous behaviors, and proactively anticipate potential security breaches as shown in Figure 3. With its adaptive nature, the xApp can continuously enhance its security protocols in response to evolving threats and dynamic network conditions, thereby fortifying the ecosystem's security framework against a spectrum of cyber threats [9].

2) Distributed Security to individual xApps: The alternative approach, known as distributed security, divides security responsibilities across multiple xApps in the ecosystem. By handing each xApp the responsibility for administering its own security procedures, reliance on a single central component is reduced. This strategy aims to enhance system autonomy and flexibility by allowing individual xApps to tailor security protocols to their specific requirements. Distributed security can be implemented practically by creating shared security libraries or modules that enable xApps to implement consistent security measures across the network. By sharing security responsibilities, each xApp gains a degree of independence in managing its security components, facilitating customization based on unique capabilities and needs. This approach

xApp Security Strategy	Strengths	Weaknesses	Synergies
Centralized Security xApp	• Unified and Consistent Security Policy Enforcement Across All xApps • Easier Management and Maintenance. • Advanced Security Analytics and Threat Detection can be applied.	• Single point of failure if the centralized security component is compromised. • Continuous Monitoring and Adaptation.	• When combined with decentralized measures, centralized security creates a defense-in-depth approach by establishing baseline security principles that decentralized security may build on.
Distributed Security to individual xApps	• Reduces the attack exposure by spreading security functions among numerous xApps. • Enables more precise and context-specific security controls. • Enhances resilience because a breach in one xApp does not affect the entire system.	• Requires more coordination and consistency across xApps to ensure coherent security policies. • Potential for security gaps if xApps do not implement security controls properly.	• Improper implementation of security measures in xApps may result in vulnerabilities. • Requires more coordination and consistency among xApps to provide consistent security policies.
xApp Repository Function XRF	• Provides scalable authentication, authorization, and discovery for xApps • Manages xApp metadata and secure API transactions. • Efficiently scales in Kubernetes microservices, supporting numerous clients with low overhead.	• Lack of specificity in handling xApp authentication and authorization at large scale. • Creates a reliance on the near-RT RIC as an authorization server, which may pose security risks.	• Centralized security can use XRF to implement consistent security standards across RIC. • XRF enables decentralized security within xApps by coordinating responses and sharing threat intelligence.

TABLE I: Here is a comparison of the strengths, weaknesses, and synergies of the centralized, decentralized, and XRF security strategies for xApps:

encourages the creation of a more adaptive security framework capable of meeting the varying needs of various xApps. Organizations can create a scalable and versatile security architecture that combines centralized coordination and distributed autonomy to address a wide range of operational needs across multi-application platforms while also effectively safeguarding the ecosystem against potential threats by incorporating elements of the hybrid model.

3) xApp Repository Function (XRF): The XRF framework ensures scalable authentication, authorization, and discovery for xApps in the O-RAN architecture through a microservice-based client-to-server augmentation. It provides a secure service discovery mechanism, facilitates efficient interaction of xApps in a microservice architecture, and distributes access tokens to xApps, enabling them to provide and consume services through secure application programming interface (API) transactions. The XRF framework is built using proven and robust concepts tested in mobile app ecosystems, compatible with the containerized microservice model, offering seamless operational security for xApps. It utilizes the Open Authorization (OAuth) 2.0 standard for authorization distribution rights and access tokens, ensuring secure service requests and validation. Additionally, the XRF framework employs sidecar proxies and a service mesh to abstract non-functional requirements from the main application, providing security, monitoring, load balancing, and other platform abstractions. The XRF server runs a multi-threaded Hypertext Transfer Protocol (HTTP) server with distinct endpoint handlers to handle the lifecycle operations of a client, ensuring efficient scalability in a multi-threaded environment under the microservice model of deployment. Overall, the XRF framework addresses the fundamental system security requirements for xApps within the O-RAN architecture by providing a comprehensive and scalable authentication, authorization, and discovery mechanism.

To ensure secure interactions and access control mechanisms, the XRF framework specifically addresses authentication, authorization, and discovery functions for xApps within the network environment. Security xApps are dedicated applications focused on enhancing network security through threat detection and mitigation. Figure 3 illustrates that by integrating these solutions, enterprises can enhance their security protocols by proactively identifying potential risks and ensuring secure access control mechanisms for xApps in the O-RAN network. Table I compares xApp security approaches, revealing a wide landscape of strengths, weaknesses, and possible synergies.

V. Conclusions and Open Research Questions

In conclusion, this paper has conducted a comprehensive evaluation of xApps and their associated security implications within the context of Next-Generation O-RAN. The exploration of the underpinnings of xApps and their integral role in enhancing network functionalities has underscored potential vulnerabilities. These vulnerabilities could allow malicious applications to compromise sensitive user data, manipulate network behavior, and disrupt network operations if not appropriately developed or configured. To counter these vulnerabilities and alleviate associated risks, we have proposed a range of risk mitigation strategies. These include secure authentication mechanisms for xApp access to RIC APIs, continuous monitoring of xApp behavior via anomaly detection systems, and encryption to protect data transmissions between xApps and the RIC.

Furthermore, we have introduced security strategies such as centralized security, distributed security, and the implementation of the XRF framework to effectively mitigate risks. By understanding xApps, acknowledging their vulnerabilities, and proposing possible efficacious risk mitigation strategies, stakeholders in the O-RAN ecosystem can bolster the security posture of their networks and safeguard the integrity and confidentiality of user data and network operations. As we move forward, continued research and development in the field of xApp security will be indispensable to adapt to emerging threats and protect the next generation of O-RAN.

ACKNOWLEDGMENT

This research work has been partially funded through the German Federal Ministry for Economy and Climate Protection (BMWK) under the project ”CampusOS” (01MC22001P/01MC22002B). The authors are responsible only for the content of this paper.

REFERENCES

[1] M. Polese, L. Bonati, S. D’oro, S. Basagni, and T. Melodia, “Understanding o-ran: Architecture, interfaces, algorithms, security, and research challenges,” *IEEE Communications Surveys & Tutorials*, 2023.

[2] T. O. Atalay, S. Maitra, D. Stojadinovic, A. Stavrou, and H. Wang, “Securing 5g openran with a scalable authorization framework for xapps,” in *IEEE INFOCOM 2023-IEEE Conference on Computer Communications*, pp. 1–10, IEEE, 2023.

[3] O-RAN Work Group 3, “Near-RT RIC Architecture,” Tech. Rep. O-RAN.WG3.RICARCH-R003-v05.00, O-RAN ALLIANCE e.V., 2023.

[4] O-RAN Work Group 11 (Security Work Group), “Study on Security for Near Real Time RIC and xApps,” Tech. Rep. O-RAN.WG11.Security-Near-RT-RIC-xApps-TR.0-R003-v05.00, O-RAN ALLIANCE e.V., 2024.

[5] 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 Journal of the Communications Society*, 2024.

[6] N. N. Sapavath, B. Kim, K. Chowdhury, and V. K. Shah, “Experimental study of adversarial attacks on ml-based xapps in o-ran,” in *GLOBECOM 2023-2023 IEEE Global Communications Conference*, pp. 6352–6357, IEEE, 2023.

[7] H. Djuitcheu, P. Kakani, H. D. Schotten, D. Brunke, and D. Fraunholz, “Exploring the Implications and Methodologies of Securing the E2 Interface,” Feb. 2024.

[8] Z. SHAHBAZI, “Analysis of security at the near-real-time ric xapps based on o-ran-defined use cases,” 2022.

[9] 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,” *arXiv preprint arXiv:2401.07643*, 2024.