Zero Trust Security Architecture for 6G Open Radio Access Networks (ORAN)

Hajar Moudoud, *Member, IEEE*, Zakaria Abou El Houda, *Member, IEEE*,
and Bouziane Brik, *Senior Member, IEEE*

***Abstract*—The evolution of Open Radio Access Networks (O-RAN) is crucial for the deployment and operation of 6G networks, providing flexibility and interoperability through its disaggregated and open architecture. However, this openness introduces new security issues. To address these challenges, we propose a novel Zero-Trust architecture tailored for ORAN (ZTORAN). ZTORAN includes two main modules: (1) A blockchain-based decentralized trust management system for secure verification, authentication, and dynamic access control of xApps; and (2) A threat detection module that uses Federated Multi-Agent Reinforcement Learning (FMARL) to monitor network activities continuously and detects anomalies within the ORAN ecosystem. Through comprehensive simulations and evaluations, we demonstrate the effectiveness of ZTORAN in providing a resilient and secure framework for next-generation wireless networks.**

***Index Terms*—ORAN, zero-trust architecture (ZTA), authentication, access control, blockchain, federated reinforcement learning.**

I. Introduction

NEXT-GENERATION networks, such as 6G and beyond, depend on Radio Access Networks (RAN) to connect mobile devices and equipment to the core network [1], [2], [3]. As these networks evolve, they require RAN to scale massively and support increasingly diverse and complex use cases, ensuring seamless connectivity, higher data rates, and low latency. RAN is critical in enabling the capabilities and performance enhancements promised by next-generation cellular technologies. However, the traditional RAN solution falls short of meeting the current 5G network requirements. These networks require high scalability, flexibility, and support for diverse and complex use cases, which traditional RANs struggle to provide. Traditional RANs are often limited by vendor lock-in, lack of interoperability, and rigid architecture, making it challenging to achieve the seamless connectivity, high data rates, and low latency essential for 6G. Therefore, the next generation of RAN is looking to open the interfaces in the RAN ecosystem. This approach, known as Open RAN, aims to disaggregate hardware and software, fostering a more competitive and innovative environment [4], [5]. However, the deployment of Open RAN introduces new security concerns. With the integration of components from multiple vendors, the complexity of the network increases, potentially creating more vulnerabilities and points of entry for malicious attacks. Ensuring the interoperability of various components while maintaining robust security protocols becomes a significant challenge. Several studies have started investigating the security challenges with the ORAN ecosystem [6], [7], [8], [9]. Among them, some studies have investigated the potential of Zero Trust to enhance the security of ORAN by addressing their inherent vulnerabilities [10]. In a traditional network, devices and users inside the network perimeter are often considered trustworthy, which can lead to significant security risks if an attacker gains access. Zero Trust, on the other hand, operates on the principle that no entity, whether inside or outside the network, should be trusted by default. By requiring continuous verification of all devices and users attempting to access network resources, Zero Trust ensures that only authenticated and authorized entities are granted access. This reduces the risk of unauthorized access and lateral movement within the network, even if an attacker penetrates the perimeter. In this context, this letter proposes ZTORAN, a novel Zero-Trust architecture tailored for the ORAN environment. ZTORAN ensures the integrity and trustworthiness of xApps within the ORAN ecosystem by enabling secure verification and authentication processes, preventing unauthorized access from malicious entities. Additionally, this module introduces a dynamic, decentralized access control mechanism, allowing vendors to manage permissions in a flexible, scalable, and secure manner. In this letter, we first describe our system model in Section II. Then, we present the implementation of ZTORAN in Section III. Finally, Section IV concludes this letter.

II. System Model

In this section, we present the core building of ZTORAN. Given the dynamic nature of the ORAN nodes, we use a Non-Real-Time RAN Controller (Non-RT RIC) as the decision center to detect intrusion. This is due to the capability of Non-RT RIC to handle complex analytics and long-term data processing (see Fig. 1). ZTORAN includes the following two main modules.

A. Decentralized Zero-Trust Framework

Zero Trust security is founded on the principle that no device or user, whether internal or external, should

Received 10 October 2024; revised 20 November 2024; accepted 2 December 2024. Date of publication 9 December 2024; date of current version 30 January 2025. This work was supported in part by the Competitive Research Project at Sharjah University, UAE, through the DeepORAN Project under Grant 2402150256, and in part by UMR INRS-UQO. The associate editor coordinating the review of this article and approving it for publication was H. Chergui. *(Corresponding author: Hajar Moudoud.)*

Hajar Moudoud is with the Département d'informatique et d'ingénierie, Université du Québec en Outaouais, Gatineau, QC J8X 3X7, Canada (e-mail: hajar.moudoud@uqo.ca).

Zakaria Abou El Houda is with INRS-EMT, UMR INRS-UQO, University of Quebec, Montreal, QC H3T 1J4, Canada (e-mail: zakaria.abouelhouda@inrs.ca).

Bouziane Brik is with the Computer Science Department, College of Computing and Informatics, Sharjah University, Sharjah, UAE (e-mail: bbrik@sharjah.ac.ae).

Digital Object Identifier 10.1109/LNET.2024.3514357

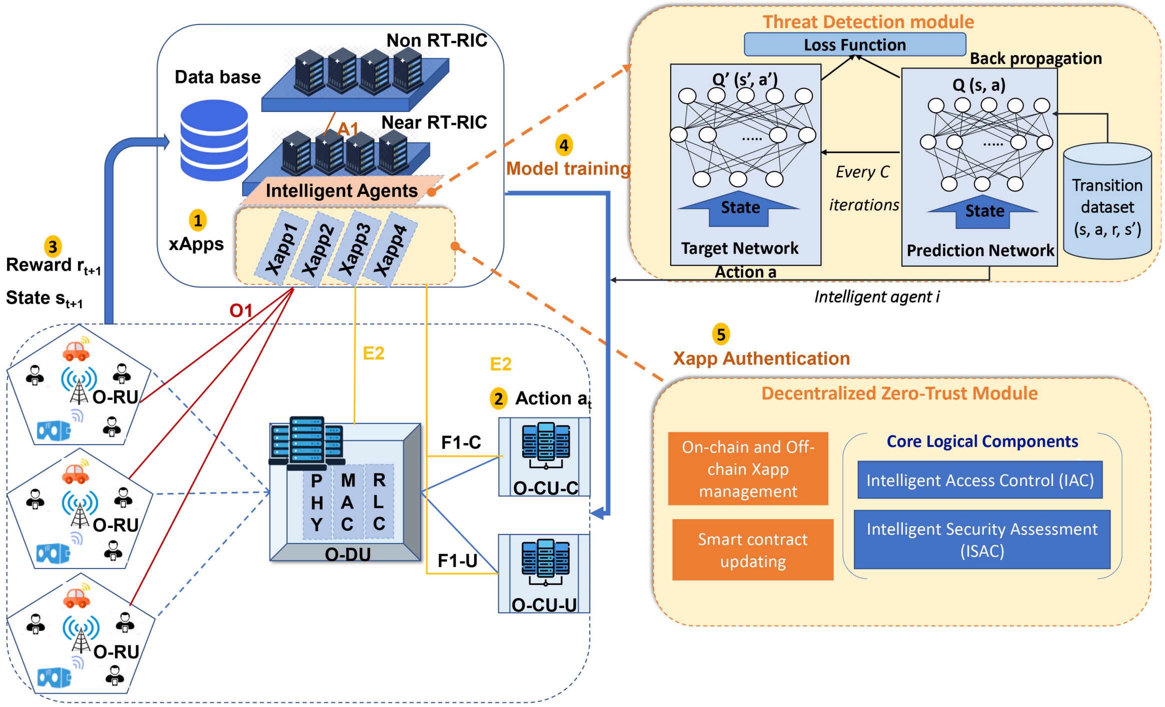


Fig. 1. ZTORAN System Architecture.

be automatically trusted. This security strategy is particularly advantageous for ORAN due to its robust protection against diverse threats, as it aligns with the blockchain-based Zero-Trust Framework (BZT-IoT) outlined in IEEE Std 3219-2023 [13]. Within a Zero Trust Architecture (ZTA), access to critical resources such as data, devices, and services is granted exclusively to authenticated and authorized entities. This model emphasizes identity verification and bases access permissions on dynamic, context-aware policies, as highlighted by the framework's focus on Policy Decision Points (PDP) and Policy Enforcement Points (PEP) for access control. The key components of ZTORAN are (1) Intelligent Access Control (IAC), corresponding to PDP and PEP, which dynamically adjusts access permissions based on the user's identity, device, and behavior, making real-time decisions to enhance security; and (2) Intelligent Security Assessment (ISAC), aligned with Continuous Security Validation and Security Information Exchange, which uses FMARL to enhance threat detection within ORAN. For IAC, we propose a system where a vendor manages xApp access at the near-RT RIC level using Access Control Contracts (ACCs), implemented as Smart Contracts on the blockchain. Each ACC governs access to specific xApps, with tuples specifying subject-object pairs, permissions, time validity, and access tokens. The system ensures secure access by verifying access tokens at the PEP using time validity and cryptographic signatures, thereby adhering to the standard's Identity Management and Policy Administration provisions. Multiple tuples manage multiple object resources for a subject, and the time-bound access tokens prevent replay attacks by embedding essential information. Mutual identity authentication between Control xApp (CxApp) and Protected xApp (PxApp) is achieved through cryptographic signatures and validity checks, leveraging the IoT Trust Service (ITS) and Smart Contract Engine (SCE) components of the framework. In our proposed access control functions, we have included operations to add/remove xApps, manage access policies, and generate tamper-proof access tokens. These functions collectively enhance security, trust, and control in the ORAN ecosystem, providing strict and verifiable access privileges to xApps while managing all xApp metadata off-chain in alignment with Log Management practices.

B. Threat Detection Module

Threat Detection module uses FMARL to enhance threat detection capabilities. By deploying local MARL agents at Near-RT RICs, this module continuously monitors network activities and performance metrics to identify anomalies. The federated learning approach preserves data privacy by aggregating model insights rather than raw data, while reinforcement learning optimizes detection strategies based on evolving network conditions. Upon detecting anomalies, the system communicates control actions to Central Units (CUs) and Distributed Units (DUs) through the E2 interface, ensuring timely responses to potential threats (see steps 1, 2, 3, and 4 in Fig. 1).

1) Deep Q-Learning: Deep Q-Learning (DQN) extends traditional Q-Learning by using deep neural networks to approximate the action-value function $Q(s, a)$. This approach is suited for high-dimensional state spaces, such as those encountered in ORAN.

In DQN, the action-value function $Q(s, a)$ is approximated using a neural network parameterized by weights θ:

$$Q(s, a; \theta) \approx Q^*(s, a) \tag{1}$$

where $Q^*(s, a)$ is the true action-value function. The goal is to minimize the difference between the predicted Q-values and the target Q-values derived from the Bellman equation. The loss function is defined as:

$$\text{Loss} = \mathbb{E}_{(s,a,r,s')\sim\mathcal{D}}\left[\left(r + \gamma \max_{a'} Q\big(s', a'; \theta^-\big) - Q(s, a; \theta)\right)^2\right] \tag{2}$$

where $\mathcal{D}$ is the experience replay buffer, θ are the parameters of the main network, θ^- are the parameters of the target network, γ is the discount factor, and r is the immediate reward received after taking action a in state s and transitioning to state s'.

Experience replay stores experiences (s, a, r, s') in a replay buffer $\mathcal{D}$. During training, random samples from $\mathcal{D}$ are used to train the network. The target Q-value y for a given sample is computed as:

$$y = r + \gamma \max_{a'} Q\big(s', a'; \theta^-\big) \tag{3}$$

The target network is updated periodically to stabilize training. The loss function for updating the main network is:

$$\text{Loss} = \mathbb{E}_{(s,a,r,s')\sim\mathcal{D}}\Big[(y - Q(s, a; \theta))^2\Big] \tag{4}$$

where y is the target value as computed above. The policy is derived from the action-value function as follows. In ϵ-greedy action selection With probability ϵ**, select a random action a. With probability $1 - \epsilon$**, select the action a that maximizes the Q-value:

$$a = \arg\max_{a} Q(s, a; \theta) \tag{5}$$

where ϵ is a parameter that decays over time to balance exploration and exploitation.

The Q-values are updated using the Bellman equation. For a given experience (s, a, r, s'), the Q-value update rule is:

$$Q(s, a; \theta) \leftarrow Q(s, a; \theta) + \alpha\left[r + \gamma \max_{a'} Q\big(s', a'; \theta^-\big) - Q(s, a; \theta)\right] \tag{6}$$

where α is the learning rate.

The target network parameters θ^- are updated periodically by copying the parameters from the main network. These updates help stabilize the learning process by providing a consistent target for Q-value estimation.

2) FMARL: In FMARL, each agent independently monitors network security and detects intrusions. Each agent trains a shared DQN using their local data and then shares the model updates with a central server. The central server aggregates these updates to construct a global model, which is redistributed to all agents. Considering N distributed clients $i = 1, 2, \ldots, N$, and a central Non-RT RIC server.

The parameter update mechanism for the local policy is described as follows:

$$\theta_i \leftarrow \theta_i + \alpha \nabla_{\theta_i} \sum_{t=1}^{T_i} \Big(r_{i,t} + \gamma \max_{a} Q_{\theta_i}\big(s'_{i,t}, a\big) - Q_{\theta_i}(s_{i,t}, a_{i,t})\Big), \tag{7}$$

where $Q_{\theta_i}(s, a)$ denotes the action-value function parameterized by θ_i, $a_{i,t}$ represents the action taken by client i at time t, ∇_{θ_i} is the gradient of the local policy, α is the learning rate, and γ is the discount factor.

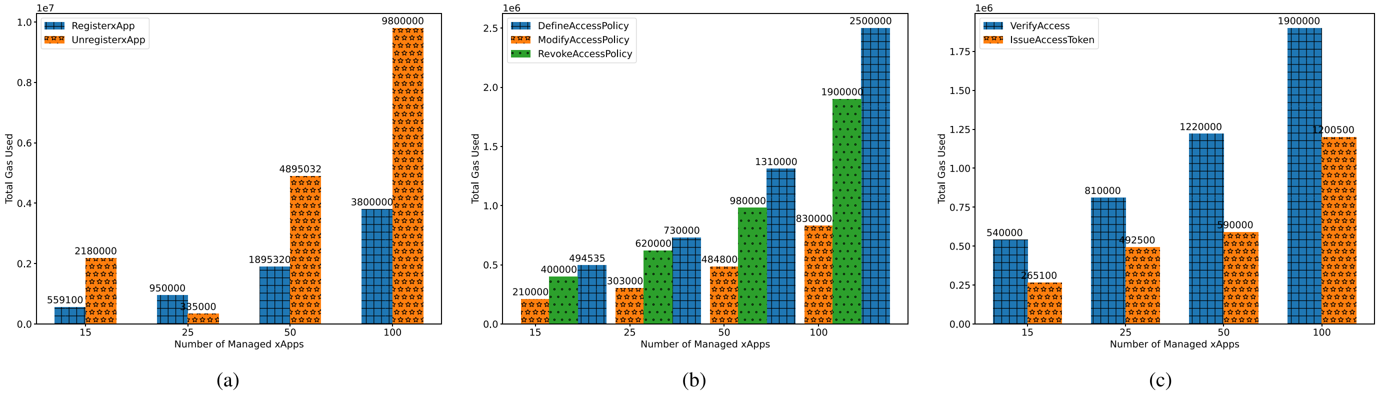
Upon completion of local training, the central server aggregates the parameters from all local policies to create the global policy p by averaging the parameters:

$$\theta = \frac{1}{N} \sum_{i=1}^{N} \theta_i, \tag{8}$$

where θ represents the parameters of the global policy. This global model is then distributed back to all clients, allowing the entire system to benefit from the collective knowledge while ensuring the privacy of individual datasets.

III. Implementation

In our implementation, we integrated ZTORAN into the ORAN ecosystem using the OSC's Kubernetes-based Near-RT RIC implementation [11]. We implemented our Access control functionalities using the Polygon Blockchain. These functions include RegisterApplication and UnregisterApplication for managing xApps, DefineAccessPolicy, ModifyAccessPolicy, and RevokeAccessPolicy for controlling resource permissions, and VerifyAccess and IssueAccessToken for ensuring secure and tamper-proof access to resources. This decentralized approach ensures that only authenticated xApps have access to network resources, with permissions that can be managed flexibly and securely. The real-world traffic attack analysis was conducted to test the efficiency of our second module (FMARL) using the WSN-DS dataset [12]. To evaluate ZTORAN, we have considered several metrics, including Accuracy and F1 Score. We have also used confusion matrices and the Receiver operating characteristic (ROC) curves. We have also evaluated the efficiency of ZTORAN in terms of flexibility and cost-effectiveness. Fig. 2 shows the gas cost analysis for ZTORAN operations across different numbers of managed xApps, ranging from 5 to 100. The experiments, with a gas price of 1 Gwei and 1 ether valued at 0.49 USD, revealed that managing 100 xApps incurs a maximum cost of 12 USD for adding or removing xApps. This demonstrates that ZTORAN is a cost-effective solution for robust and secure access control in large-scale ORAN deployments, enhancing the ecosystem's security and trustworthiness. ZTORAN provides dual-level flexibility for the ORAN ecosystem. First, it enables ORAN vendors to easily add or remove trusted xApps using RegisterApplication() and UnregisterApplication(), and to manage access policies through DefineAccessPolicy(), ModifyAccessPolicy(), and RevokeAccessPolicy(). This capability allows for dynamic adjustments to evolving needs. Second, ZTORAN facilitates seamless vendor participation and exit from the ecosystem, ensuring smooth interoperability and adaptability. These features collectively improve the efficiency, scalability, and agility of the ORAN network. To test the efficiency of our FMARL detection module we have varied the number of training rounds from 10 to 50. Fig. 3 shows the confusion matrix and ROC curve. Our FMARL detection

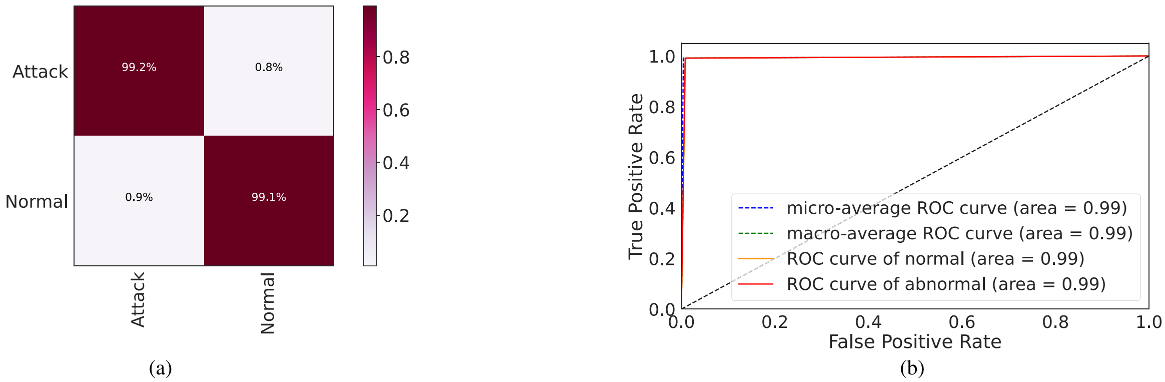


(a)

(b)

(c)

Fig. 2. Gas Cost Analysis for ZTORAN Operations Across Different Numbers of Managed xApps Functions.



(a)

(b)

Fig. 3. Performance Evaluation of ZTORAN in terms (a) confusion matrix; and (b) ROC curve.

module achieves high accuracy and F1 scores, both reaching a score of 99%.

IV. Conclusion

This letter proposed a decentralized Zero-Trust Framework using blockchain technology for secure authentication and dynamic access control, and a Threat Detection module with FMARL for privacy-preserving anomaly detection. For future works, we intend to develop more advanced access management strategies that analyze contextual information (such as user location, device type, and network conditions) to enhance access control mechanisms and to study the trade-offs between security and model performance. Also, we intend to analyze how adding or removing xApps impacts connectivity times between the CxApp and PxApp or the near-RT RIC and any xApp to optimize system performance.

References

[1] P. Schwenteck, G. T. Nguyen, H. Boche, W. Kellerer, and F. H. P. Fitzek, "6G perspective of mobile network operators, manufacturers, and verticals," *IEEE Netw. Lett.*, vol. 5, no. 3, pp. 169–172, Sep. 2023, doi: 10.1109/LNET.2023.3266863.

[2] M. Corici, F. Eichhorn, and T. Magedanz, "Organic 6G continuum architecture: A uniform control plane across devices, radio, and core," *IEEE Netw. Lett.*, vol. 6, no. 1, pp. 11–15, Mar. 2024, doi: 10.1109/LNET.2023.3338363.

[3] M. Polese et al., "Empowering the 6G cellular architecture with open RAN," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 2, pp. 245–262, Feb. 2024, doi: 10.1109/JSAC.2023.3334610.

[4] S. Roy, H. Chergui, and C. Verikoukis, "Toward bridging the FL performance-explainability tradeoff: A trustworthy 6G RAN slicing use-case," *IEEE Trans. Veh. Technol.*, vol. 73, no. 7, pp. 10529–10538, Jul. 2024, doi: 10.1109/TVT.2024.3364363.

[5] N. Ghafouri, J. S. Vardakas, K. Ramantas, and C. Verikoukis, "A multi-level deep RL-based network slicing and resource management for O-RAN-based 6G cell-free networks," *IEEE Trans. Veh. Technol.*, vol. 73, no. 11, pp. 17472–17484, Nov. 2024, doi: 10.1109/TVT.2024.3415656.

[6] 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, doi: 10.1109/COMST.2023.3239220.

[7] J. Groen et al., "Securing ORAN open interfaces," *IEEE Trans. Mobile Comput.*, submitted for publication, doi: 10.1109/TMC.2024.3393430.

[8] Z. A. E. Houda, H. Moudoud, and B. Brik, "Federated deep reinforcement learning for efficient jamming attack mitigation in O-RAN," *IEEE Trans. Veh. Technol.*, vol. 73, no. 7, pp. 9334–9343, Jul. 2024, doi: 10.1109/TVT.2024.3359998.

[9] H. Moudoud and S. Cherkaoui, "Enhancing open RAN security with zero trust and machine learning," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, 2023, pp. 2772–2777, doi: 10.1109/GLOBECOM54140.2023.10437043.

[10] H. Jiang, H. Chang, S. Mukherjee, and J. Van der Merwe, "OZTrust: An O-RAN zero-trust security system," in *Proc. IEEE Conf. Netw. Funct. Virtualization Softw. Defin. Netw. (NFV-SDN)*, 2023, pp. 129–134, doi: 10.1109/NFV-SDN59219.2023.10329620.

[11] "Non-RealTime RIC." 2024. [Online]. Available: https://lf-o-ran-sc.atlassian.net/wiki/spaces/RICNR/overview

[12] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks," *J. Sens.*, no. 1, 2016, Art. no. 4731953.

[13] *IEEE Standard for Blockchain-Based Zero-Trust Framework for the Internet of Things (IoT)*, IEEE Standard 3219-2023, Apr. 2024, doi: 10.1109/IEEESTD.2024.10531234.