Blockchain Meets O-RAN: A Decentralized Zero-Trust Framework for Secure and Resilient O-RAN in 6G and beyond

Zakaria Abou El Houda[1], Hajar Moudoud[2], and Lyes Khoukhi[3]

[1]Institut National de la Recherche Scientifique (INRS-EMT), Varennes (Quebec), Canada
[2]L@bISEN, ISEN Yncrea Ouest, France
[3]Normandie Univ, ENSICAEN, UNICAEN, CNRS GREYC, 14000 Caen, France
zakaria.abouelhouda@inrs.ca, Hajar.Moudoud@usherbrooke.ca,
lyes.khoukhi@ensicaen.fr

***Abstract*—O-RAN (Open Radio Access Network) is an initiative that promotes the development of open and interoperable radio access technologies. The O-RAN Alliance has undertaken specification efforts that align with O-RAN principles, incorporating the near-real-time RAN Intelligent Controller (RIC) to manage extensible applications (xApps) owned by various ORAN operators and vendors. However, this integration of untrusted third-party applications raises significant security concerns, expanding the threat surface of 6G networks. Moreover, the heterogeneity in deployment, with apps residing on various sites, poses challenges for traditional security models based on perimeter security. To overcome this issue, a Zero Trust Architecture (ZTA) becomes paramount to ensure network security. In this context, we introduce TrustORAN, a novel blockchain-based decentralized Zero-Trust Framework designed to ensure security and trustworthiness in O-RAN. TrustORAN allows for the verification and authentication of xApps by O-RAN players, to prevent unauthorized access from malicious xApps. Moreover, we introduce a dynamic decentralized-based access control framework that allows vendors to manage permissions in a fully decentralized, flexible, scalable, and secure manner. TrustORAN architecture is implemented, tested, and deployed on both private and public blockchains. The obtained results demonstrate that TrustORAN empowers 6G O-RAN networks with heightened security, resilience, and robustness, providing effective protection against evolving security threats while ensuring Trust.**

***Index Terms*—O-RAN; Zero-Trust; authentication; authorization; security.**

I. Introduction

A Radio Access Network (RAN) is a network that links mobile devices to the core network of a mobile network operator, handling crucial radio-related tasks such as data transmission and reception through the airwaves. Open RAN (O-RAN) represents a collection of technologies and methods aimed at improving RAN openness, interoperability, and flexibility. It achieves this by adopting open interfaces, standard protocols, and open hardware and software within the RAN. This approach allows various vendors to seamlessly provide compatible equipment and software, allowing mobile network operators to easily mix and match different components in their networks. The primary objectives of ORAN are to foster increased competition, lower costs, and stimulate innovation in the RAN domain.

Despite O-RAN's potential to transform the telecoms sector, privacy and security issues remain major concerns [1], [2]. First, ORAN networks handle sensitive and confidential data, making it essential to prevent unauthorized access and protect user privacy [3]–[5]. Second, ensuring the security of ORAN enhances network resilience, preventing potential disruptions in services and maintaining seamless connectivity for users. Third, security breaches in ORAN can lead to financial losses, customer churn, and liabilities, impacting the overall economy. Additionally, as critical infrastructure, compromised ORAN networks could have severe implications for national security. Maintaining a secure ORAN environment preserves the reputation of mobile network operators, fosters customer trust, and ensures compliance with regulatory requirements. Furthermore, data integrity is crucial, and securing ORAN prevents unauthorized tampering and safeguards against potential misinformation.

Securing O-RAN using the zero-trust model can be a transformative approach for telecom operators. The goal is to ensure that every device, user, and network flow is authenticated, authorized, and continuously validated, even after initial access is granted. A zero-trust framework assumes that a breach can occur at any time, so it verifies every request as if it originates from an open network. In the context of O-RAN, this means that every device, user, and network flow should be validated in real-time. The implementation of zero trust in O-RAN can enable device authentication, user authentication, and flow validation [6]. With Device Authentication, the identity of each device attempting to join the network is verified, preventing unauthorized access and potential security breaches. Similarly, user authentication ensures that every user or automated system seeking entry is properly authenticated, mitigating the risk of unauthorized personnel gaining access. Additionally, flow validation plays a crucial role in maintaining data integrity and confidentiality. By validating and encrypting each network flow or data packet, potential threats are mitigated, ensuring that only legitimate and secure communication takes place within the network. This comprehensive approach to network security fosters a safe and protected environment, safeguarding sensitive information and preserving the O-RAN integrity.

Blockchain technology offers significant advantages to O-RAN (Open Radio Access Network) security. Firstly, it provides an immutable and tamper-resistant ledger, bolstering trust and integrity within the O-RAN network. This characteristic ensures transparent and secure communication among network participants, preventing unauthorized modifications to critical data and maintaining data integrity. Second, the decentralized nature of blockchain promotes a distributed governance model, reducing single points of failure and enhancing overall resilience in the O-RAN ecosystem. This decentralization also fosters increased transparency and accountability, as actions within the network are traceable and auditable. Lastly, blockchain's smart contracts introduce decentralized and automated access control mechanisms in the O-RAN. These self-executing contracts enable parties to establish predefined conditions and rules, automatically enforcing them without the need for intermediaries. This helps prevent unauthorized alterations to sensitive information and guarantees the integrity of interactions within the network.

In this context, we introduce TrustORAN, a novel blockchain-based decentralized Zero-Trust Framework designed to ensure the security and resilience of O-RAN in 6G and beyond. Fig. 1 shows the high-level integration of ORAN with blockchain and zero trust. TrustORAN integrates a Two-stage Authentication and Authorization Framework, utilizing Blockchain Smart Contracts to ensure secure authentication while granting Access Tokens for Authorization. TrustORAN allows the verification and authentication of xApps by O-RAN players, including ORAN operators and vendors, to prevent unauthorized access from malicious xApps, enabling O-RAN vendors to manage the authentication and authorization of their xApps in a fully decentralized, flexible and secure manner. TrustORAN architecture is implemented, tested, and deployed on both private and public blockchains. The obtained results demonstrate that TrustORAN empowers 6G O-RAN networks with heightened resilience and robustness, providing effective protection against evolving security threats.

The main contributions of this paper are summarized as follows:

- We introduce TrustORAN, an innovative blockchain-based decentralized zero-trust framework aimed at enhancing the security and resilience of O-RAN in the context of 6G and future generations.
- We design a two-stage authentication and authorization framework, utilizing blockchain smart contracts to manage the authentication and authorization of their xApps in a fully decentralized, flexible, and secure manner.
- The performance of TrustORAN is thoroughly evaluated, considering factors such as flexibility, security, cost-effectiveness, and efficiency. Our experimental results confirm that TrustORAN is a highly effective solution for enhancing the security and resilience of O-RAN.

The remainder of this paper is structured as follows. Section II presents the Zero Trust Architecture. Section III describes our system model. Section IV presents the performance evaluation. Section V concludes the paper.

II. Zero Trust Architecture

Zero trust is defined as a set of concepts and relationships between components, workflow planning, and access policies that can be used to increase the security of infrastructure in publications published in 2018 by the National Institute of Standards and Technology (NIST) and the National Cybersecurity Center of Excellence (NCCoE) [7]–[9]. According to them, zero trust must consist of three components: software-bounded perimeters, micro-segmentation, overlay networks, and improved identity governance and policy-based access restrictions. Zero trust architecture includes four components as follows:

- Access control and authentication (ACA): ACA is a crucial part of any Zero Trust blueprint, serving as the foundation for confirming the credibility of users and devices, granting permissions, and instituting access controls. It encompasses identity validation, access rules, multiple-factor authentication, and other safety measures to ensure that only vetted users and devices can avail of network resources.
- Network segmentation: The process of dividing a complex network into smaller, easier-to-manage segments and assigning access controls to each, based on the identity and behavior of users and devices, is known as network segmentation. This technique can help mitigate security risks and minimize the consequences of potential breaches. By breaking the network down into segments, access to confidential information and vital systems is limited to only approved users and devices, thereby lowering the risk of unauthorized access and data leaks.
- Monitoring and Data Analysis (MDA): MDA is vital to any Zero Trust framework, as it ensures real-time updates on network activity, user behavior, and device conditions. These elements can assist in pinpointing potential security threats and allowing for a quick response to any irregularities.
- Management of Policies: The creation and enforcement of policies that regulate the access of users and devices to network resources is part of policy management.
- Edge Service for Secure Access (ESSA): ESSA is an evolving strategy in network security that integrates network security features such as firewalls, intrusion prevention, and web filtering with secure access technologies like VPNs and multiple-factor authentication. ESSA can offer an extensive and scalable security solution for Zero Trust frameworks.

III. System Model

In this section, we first overview our system model which includes a threat model, and a control model. We then explore

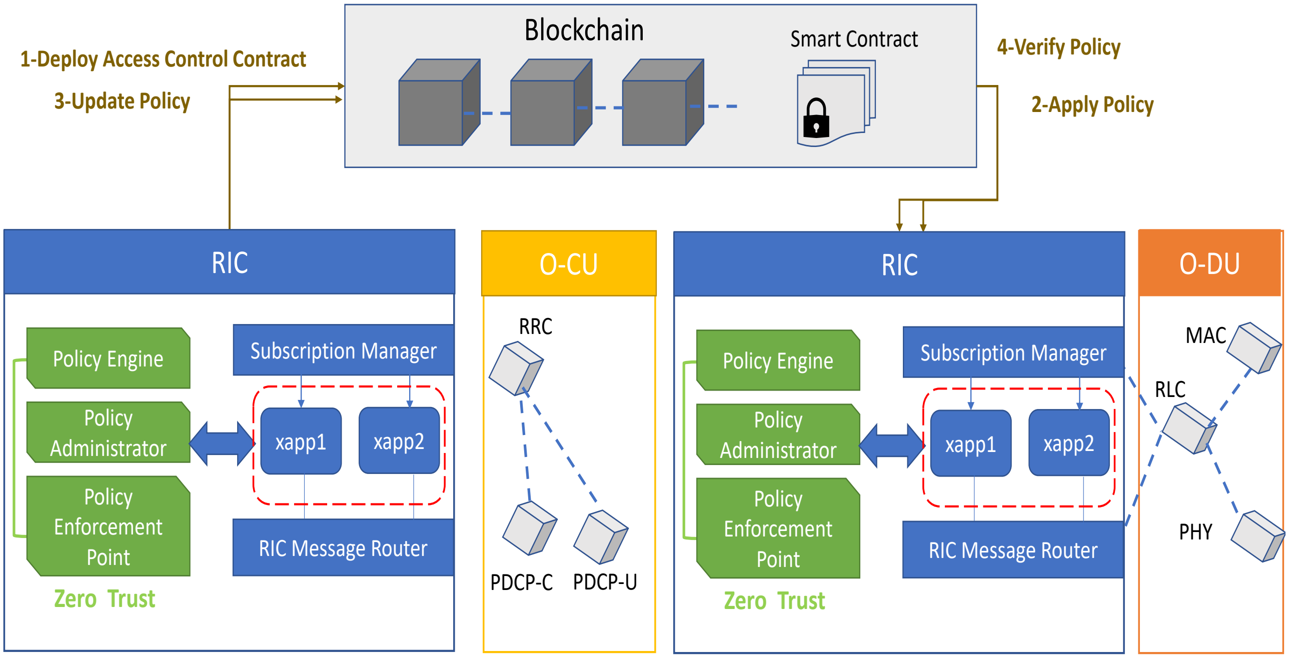


Fig. 1: High-level overview of the O-RAN with blockchain and ZTA.

how this scheme effectively ensures fully decentralized and trustworthy access control for xApps in O-RAN.

A. System Overview

1) Threat model: The O-RAN alliance has undertaken specification efforts that align with O-RAN principles, incorporating the near-real-time RAN Intelligent Controller (RIC) to manage extensible applications (xApps) owned by diverse ORAN operators and vendors. This fosters a heterogeneous network deployment by integrating xApps from different vendors. However, this integration of untrusted third-party applications raises significant security concerns, expanding the threat surface of 6G networks.

- **Untrusted Entities:** Malicious xApps aiming to exploit exposed APIs (using well-known protocols) and the absence of proper authentication and authorization mechanisms. These malicious xApps seek to compromise the security of other xApps and the near-RT RIC's internal communications, potentially leading to eavesdropping on or disrupting radio stack operations.
- **Attack Vector:** In O-RAN, the near-RT RIC (Real-Time RAN Intelligent Controller) plays a crucial role in managing xApps (applications) that could be exploited for malicious purposes. These malicious xApps may target exposed APIs using well-known protocols, taking advantage of weak authentication and authorization mechanisms. Infiltrating the ORAN ecosystem, these xApps pose a threat to the security and integrity of legitimate xApps and internal communications within the near-RT RIC. Potential risks include unauthorized access to sensitive data, interference with radio stack operations, and eavesdropping on critical network communications. The decentralized nature of ORAN networks, integrating xApps from diverse vendors, exacerbates these security concerns, challenging traditional security models. To address this, adopting advanced security measures such as ZTA becomes essential. ZTA ensures strict enforcement of authentication, authorization, and access controls for every entity in the network, regardless of its location. This approach requires continuous verification of each xApp and actor before accessing resources, providing an additional layer of security to prevent potential breaches.

2) Access control model: We propose exploring the different access control scenarios, including malicious and honest xApps and near-RT RIC, with the ability to read other xApps' data. Our proposal integrates blockchain to create a fully decentralized zero-trust architecture in the O-RAN ecosystem. Blockchain ensures tamper-proof and transparent access control policies, providing an audit trail for accountability and forensic analysis. The zero-trust architecture enhances security and trust by strictly controlling access for all entities. Each xApp maintains its own access control policies, specified by vendors, and implements smart contracts for xApp and near-RT RIC pairs. The following provides a concise summary of the key roles of the various system participants:

- **Policy Engine (PE):** The Policy Engine is responsible for enforcing and implementing the access control policies specified by the vendors for each xApp. The PE acts as a centralized or distributed entity, depending on the network architecture. It receives access requests from xApps and near-RT RIC, and based on predefined rules and policies, it grants or denies access to specific resources or functionalities within the O-RAN network. The PE ensures that access control decisions are made in real-time and align with the Zero Trust architecture principles. It collaborates with other components, such as blockchain and smart contracts, to verify and authenticate access requests securely.

- **Policy administrator (PA):** PA plays a pivotal role in managing access control policies within the O-RAN ecosystem. As a central authority, the PA defines, configures, and updates access control rules for xApps and near-RT RIC entities. To ensure security and transparency, the PA leverages blockchain technology to record and validate access control decisions in a tamper-proof and immutable manner. Blockchain integration enhances the PA's role by providing a transparent audit trail and facilitating decentralized access control management, thereby strengthening the overall trustworthiness and security of the O-RAN network.
- **Policy Enforcement Point (PEP):** PEP acts as a gatekeeper, intercepting access requests and verifying them against predefined policies set by the Policy Administrator. The PEP leverages blockchain technology to access and enforce tamper-proof access control policies, ensuring secure and reliable access decisions while maintaining data integrity and preventing unauthorized access.
- **Blockchain and ACCs:** Blockchain technology is leveraged to establish a tamper-proof and transparent record of access control contracts. Each access control contract, represented as a smart contract on the blockchain, contains predefined rules and conditions for access control for a particular xApp. Access requests made by xApps or near-RT RIC entities are verified against these contracts, ensuring that access is granted only to authorized entities [10].

B. System interaction and smart contracts

We consider a vendor ($i.e.$, contract owner/creator) that would like to manage the access to its xApps at near-RT RIC level. First, it creates multiple ACCs and deploys them in the blockchain. In our system, each Access Control Contract (ACC) is created and deployed to govern access to specific xApps. Each ACC contains a mapping for one-to-many access control for a subject-object pair. Only authenticated subjects (i.e., xApps or near-RT RIC) are authorized to access the resources of an object (i.e., xApps) during a specific time frame, effectively preventing unauthorized access by malicious xApps. In our system, each Access Control Contract (ACC) is represented as a set of tuples denoted as $ACC = \{(S_i, O_j, R_k, P_{ijk}, T_{ijk}, \text{Token}_i, \text{Validity}_i)\}$, where S_i represents the subject (e.g., xApp or near-RT RIC), O_j represents the object (e.g., xApp), R_k represents the specific resource within the object (e.g., data fields or functionalities), P_{ijk} denotes the permission granted to subject S_i to access resource R_k of object O_j, T_{ijk} represents the time validity period for this permission, Token$_i$ is the access token assigned to subject S_i for authorization, and Validity$_i$ represents the time validity of the access token Token$_i$.

To handle multiple object resources, the ACC may contain multiple tuples for each subject-object pair, encompassing all the resources that the subject is allowed to access within the object. To access the resources, the subject S_i presents the access token Token$_i$ along with its request to the Policy Enforcement Point (PEP). The PEP verifies the authenticity of the access token by checking its time validity Validity$_i$ and ensures that it is signed by the subject S_i. The signature is validated using the subject's public key, ensuring that the access token was generated by the authorized subject.

If the access token is valid, the request aligns with the specified permissions and time validity, and the signature is verified, the PEP grants the subject S_i access to the requested resources R_k, R_{k+1}, R_{k+2}, ... of object O_j. By incorporating a time validity period for the access token and requiring a signature by the subject, the system enhances the security and trustworthiness of the access control mechanism within the O-RAN ecosystem.

In our proposed system, the access token is a unique hash generated with the Solidity function "keccak256," specific to a Control xApp (CxApp). It includes a nonce to prevent replay attacks and crucial information like the CxApp's Ethereum address, Protected xApp (PxApp)'s Ethereum address, connection contract address, block timestamp, and access token validity. For mutual identity authentication, the CxApp creates a package containing the access token, its Ethereum address, PxApp's Ethereum address, and token validity, signed with the CxApp's private key. This package, along with the corresponding public key, is sent to the PxApp. The PxApp verifies the CxApp's public key, validates the signature, and checks the access token's validity. Upon successful checks, the PxApp constructs a response package signed with its private key and sends it back to the CxApp. This secure process, utilizing access tokens, cryptographic signatures, and validity checks, ensures reliable mutual authentication between the CxApp and PxApp, enhancing system security by preventing unauthorized access attempts.

We propose a set of access control functions for xApp authorization in O-RAN. The Access Control Contract (ACC) is integrated with a blockchain to establish trust and ensure a fully decentralized and secure environment. The functions include:

- **AddxApp(xApp.EOA, xApp.Infos)**: Allows the resource owner of the ACC to add xApps, ensuring only authenticated xApps are authorized.
- **RemovexApp(xApp.EOA)**: Enables the ACC owner to remove xApps from the system, subject to prior registration.
- **AddPolicy(xApp.EOA, Resource, Action, Permission, Expiration_Time)**: Add access policies to the policy list,

controlling xApp-resource access with specified permissions.

- **UpdatePolicy(xApp.EOA, Resource, Action, Permission, Expiration_Time)**: Allows the ACC owner to update existing access policies with revised permissions.
- **DeletePolicy(xApp.EOA, Resource, Action, Permission, Expiration_Time)**: Permits the removal of specific access policies for xApp-resource pairs.
- **CheckAccess(xApp.EOA, Resource, Action, Permission, Expiration_Time)**: Enables authorized xApps or ACC owner to verify access control and obtain access results.
- **GenerateAccessToken(xApp.EOA, Resource, Action, Permission, Expiration_Time)**: A function to generate tamper-proof access tokens for xApps, signed with xApp's private key and verified by the network nodes, ensuring secure and time-bound access to resources.

These functions collectively enhance security, trustworthiness, and control in the O-RAN ecosystem, empowering xApps with strict and verifiable access privileges.

IV. Evaluation

In this section, we evaluate the effectiveness of the TrustORAN scheme based on its flexibility, security, and cost-effectiveness. Additionally, we conduct a comparative analysis between our proposed scheme and other prominent approaches to evaluate its strengths and advantages.

A. Flexibility

TrustORAN offers two levels of flexibility to the ORAN ecosystem. Firstly, it empowers the ORAN vendor (*i.e.*, ACC owner/creator) with the ability to easily add or delete trusted xApps to/from the access control system using the functions `AddxApp()` and `RemovexApp()`. Additionally, the vendor can seamlessly manage access policies by employing the functions `AddPolicy()`, `UpdatePolicy()`, and `DeletePolicy()` to add, update, or remove policies as needed. This level of flexibility enables dynamic adaptation to changing requirements and environments. Second, TrustORAN allows the ORAN vendor to join or leave the ORAN ecosystem with ease. This provides the vendor with the freedom to participate in the ecosystem as needed, ensuring interoperability and adaptability. The combination of these flexibilities improves the efficiency and scalability of the ORAN network, promoting a more dynamic and agile environment.

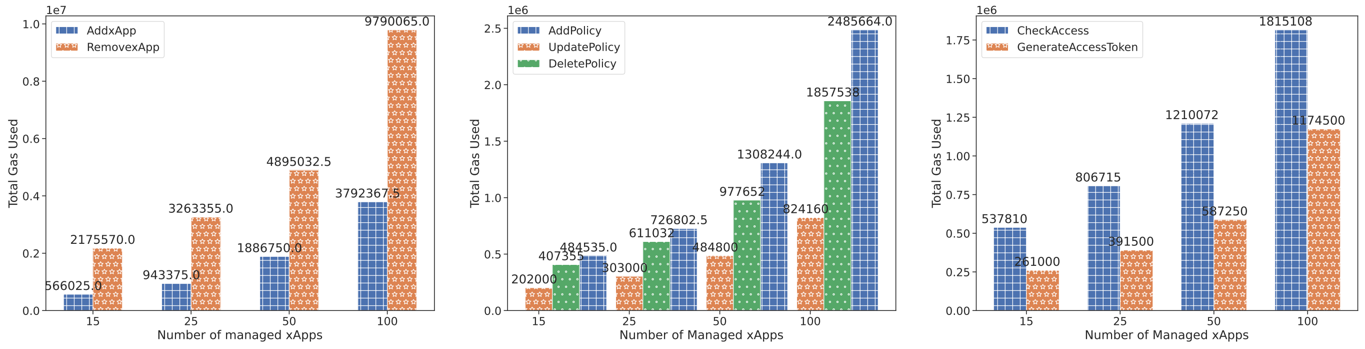
B. Security

To ensure that only authorized and authenticated xApps can access specific resources owned by the ORAN vendor, the Access Control Contract (ACC) utilizes modifiers. For instance, the "OnlyOwner" modifier restricts the execution of functions such as addxApp(), removexApp(), AddPolicy(), DeletePolicy(), and changeStatus() to only the ACC owner (xApp), preventing unauthorized attempts by malicious xApps to gain access to the ORAN vendor's resources. Any such unauthorized execution will fail, and no action will be recorded on the blockchain. Similarly, the "OnlyxApps" modifier is applied to the execution of the CheckAccessControl() function, ensuring that only xApps, along with the contract owner (xApp), have the privilege to verify if they possess access to object resources owned by the ORAN vendor. These modifiers act as security measures, enforcing strict access control rules and safeguarding the integrity and confidentiality of the O-RAN ecosystem. By employing these modifiers and blockchain technology, TrustORAN ensures that only authorized xApps can access the resources owned by the ORAN vendor, enhancing the overall security and trustworthiness of the O-RAN network.

TrustORAN utilizes blockchain technology in the O-RAN ecosystem to enhance security by preventing non-repudiation and safeguarding against man-in-the-middle attacks. The immutability and tamper-proof nature of the blockchain ensure that all access control decisions and actions are securely recorded, creating a reliable and indisputable audit trail. Through the use of blockchain-based smart contracts for access control management, TrustORAN eliminates the need for a central authority, thereby reducing the risk of man-in-the-middle attacks. Smart contracts, executed on a decentralized blockchain network, validate access control decisions through consensus among network nodes, making it extremely difficult for attackers to manipulate or forge access control data. Additionally, TrustORAN employs digital signatures in the generation and verification of access tokens. When an xApp requests access to resources, it signs the access token with its private key, including essential information such as Ethereum addresses, connection contract details, block timestamp, and access token validity. The Access Control Component (ACC) then verifies the digital signature using the xApp's public key, ensuring the authenticity and integrity of the access token.

C. Cost Effectiveness

We examine the costs associated with the functions implemented in TrustORAN, as depicted in Fig. 2. The experiments conducted to analyze these costs utilized a specific gas price of $1Gwei$, where $1Gwei$ is equivalent to 10^9 wei, and 1 ether was valued at 1800 USD. Fig. 3 illustrates the Gas Costs of TrustORAN Creation and Functions for varying numbers of managed xApps, ranging from 5 to 100. In particular, with 100 managed xApps, the cost of adding or removing xApps reaches a maximum of 20 USD. Additionally, when dealing with 100 managed xApps, adding, updating, or removing access control rules incurs costs of 4 USD, while the check access function costs just 0.108 USD per xApp. The overall costs associated with all functions provided by the ACC remain low. Therefore, we can conclude that TrustORAN deployment is cost-effective, rendering it a promising framework for robust and secure access control in the context of O-RAN. Fig. 3 illustrates a quantitative performance comparison with a recent study that used the OAuth2 protocol for scalable access control in O-RAN, named XRF. We observe that TrustORAN achieves high scalability, a lightweight design, user-friendliness, flexibility,



(a) (b) (c)

Fig. 2: Gas Costs of TrustORAN Creation and Functions under Various Numbers of Managed xApps Functions: a) Deployment Costs of AddxApp and RemovexApp; b) Deployment Costs of AddPolicy, UpdatePolicy, and DeletePolicy; and c) Deployment Costs of CheckAccess and GenerateAccessToken.

and cost-effectiveness. These outstanding attributes position TrustORAN as a promising framework for ensuring secure O-RAN communication.

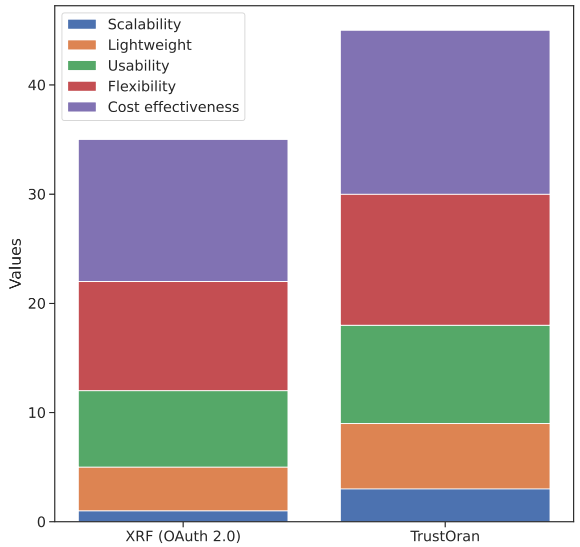


Fig. 3: Quantitative evaluation of the Blockcahin-bsed solution and TrustORAN.

V. Conclusion

The O-RAN initiative promotes open and interoperable radio access technologies. Integration of untrusted third-party applications raises significant security concerns in 6G networks, challenging traditional perimeter security models. To address this, we proposed TrustORAN, a novel blockchain-based decentralized Zero-Trust Framework designed to ensure security and trustworthiness in O-RAN. TrustORAN allowed verification and authentication of xApps to prevent unauthorized access. Furthermore, our dynamic decentralized access control framework enables vendors to manage permissions in a secure, scalable, and flexible manner. TrustORAN was deployed on private and public blockchains, providing heightened security and resilience to 6G O-RAN networks, while also ensuring trust in the system.

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*, vol. 25, no. 2, pp. 1376–1411, 2023.

[2] L. Giupponi and F. Wilhelmi, "Blockchain-enabled network sharing for o-ran in 5g and beyond," *IEEE Network*, vol. 36, no. 4, pp. 218–225, 2022.

[3] 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*, 2023, pp. 1–10.

[4] Z. A. El Houda, H. Moudoud, B. Brik, and L. Khoukhi, "Securing federated learning through blockchain and explainable ai for robust intrusion detection in iot networks," in *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2023, pp. 1–6.

[5] Z. A. E. Houda, H. Moudoud, and B. Brik, "Federated deep reinforcement learning for efficient jamming attack mitigation in o-ran," *IEEE Transactions on Vehicular Technology*, pp. 1–10, 2024.

[6] H. Sedjelmaci and K. Tourki, "A distributed zero trust framework for 6g ran," in *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, 2023, pp. 1–5.

[7] I. A. Ridhawi, S. Otoum, and M. Aloqaily, "Decentralized zero-trust framework for digital twin-based 6g," 2023.

[8] 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 Network*, vol. 36, no. 6, pp. 206–213, 2022.

[9] S. D'Oro, L. Bonati, M. Polese, and T. Melodia, "Orchestran: Network automation through orchestrated intelligence in the open ran," in *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, 2022, pp. 270–279.

[10] Z. A. E. Houda, H. Moudoud, B. Brik, and L. Khoukhi, "Blockchain-enabled federated learning for enhanced collaborative intrusion detection in vehicular edge computing," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–0, 2024.