ABElity: Attribute Based Encryption for Securing RIC Communication in Open RAN

K Sowjanya
Indian Institute of Technology Delhi
sowjanya.kandisa@gmail.com

Rahul Saini
Eindhoven University of Technology
r.saini@tue.nl

Dhiman Saha
Indian Institute of Technology Bhilai
dhiman@iitbhilai.ac.in

Kishor Joshi
Eindhoven University of Technology
k.c.joshi@tue.nl

Madhurima Das
Indian Institute of Technology Delhi
madhurimadasisme@gmail.com

***Abstract*—The A1 and R1 interfaces in Open Radio Access Networks (O-RAN) play crucial roles in facilitating RAN Intelligent Controller (RIC) communication within the RAN ecosystem. The A1 interface enables high-level policy communication between the Non-Real-Time RIC (Non-RT RIC) and the Near-Real-Time RIC (Near-RT RIC), while the R1 interface connects rApps with the Non-RT RIC to support intelligent RAN operations. Current implementations of both interfaces primarily rely on Transport Layer Security (TLS) to ensure secure communication and Role Based Access Control (RBAC) for authorization. However, the evolving landscape of cyber threats and the movement towards Zero-Trust Architecture (ZTA) demands more advanced security mechanisms. This paper explores the integration of Attribute-Based Encryption (ABE) as a security enhancement for both A1 and R1 communications. ABE offers fine-grained access control by leveraging attributes, providing greater security and flexibility compared to traditional methods. We present a comprehensive threat model, justify the adoption of ABE, and evaluate its advantages over existing solutions. Additionally, we propose a novel ABE-based framework tailored to the A1 and R1 interfaces, emphasizing its scalability, efficiency, and suitability for dynamic and distributed O-RAN environments.**

I. Introduction

The advent of Open Radio Access Networks (O-RAN) has transformed telecommunications by embracing modularity, interoperability, open interfaces, and intelligent RAN operations. One of key components in O-RAN is considered to be both the RAN Intelligent Controllers (RICs), namely Near Realtime RIC (Nr-RT RIC) and Non Realtime RIC (Non-RT RIC). The control loop for Nr-RT RIC is between $10ms$ and $1s$. However, for non-RT RIC it is more than $1s$. The application running in Nr-RT RIC are known as xApps, and for Non-RT RIC these are called rApps. These applications are used for automation and intelligent decision making based on deployment scenarios. These two RICs are connected using the A1 interface. The A1 interface performs a critical task in communicating policies and is vital for the transmission of intents from the Non-RT RIC to the Nr-RT RIC [1], while the R1 interface enables communication between rApps and the Non-RT RIC framework to support advanced RAN policies and functionalities [2]. O-RAN transforms telecommunications by optimizing RAN operations through virtualization, disaggregation, open interfaces, and AI-driven intelligence. **virtualization** decouples network functions from hardware for flexibility, while **disaggregation** enables interoperable multi-vendor solutions. **open interfaces** standardize RAN, fostering innovation and reducing vendor lock-in. **AI/ML** enhances efficiency and adaptability, creating cost-effective, customizable, and future-ready networks.

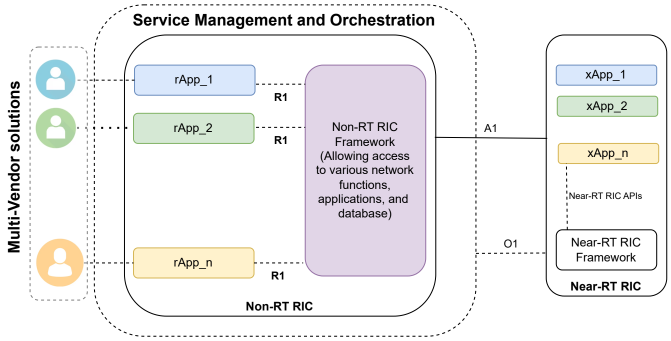

Service Management and Orchestration
Multi-Vendor solutions
rApp_1
rApp_2
rApp_n
R1
R1
R1
Non-RT RIC Framework (Allowing access to various network functions, applications, and database)
Non-RT RIC
A1
O1
xApp_1
xApp_2
xApp_n
Near-RT RIC APIs
Near-RT RIC Framework
Near-RT RIC

Fig. 1. Multi-vendor based Non-RT RIC

The A1 and R1 interfaces are highly critical for communication between RIC frameworks. These two interfaces provide a communication link for managing RAN resources and policies for performance and optimization. The rApp uses R1 interface for communication with Non-RT RIC platform framework for various data-driven requirements. Once the policies or operation parameters are formalized, they can be communicated using the A1 interface to Nr-RT RIC, where xApps can take advantage of the policies in near real-time decision making [3]. Transformation in RAN to make it more transparent and intelligent has its benefits, allowing innovation through competition among vendors is beneficial as illustrated in Fig. 1. However, the openness of O-RAN also brings about

Workshop on Security and Privacy of Next-Generation Networks
(FutureG) 2025
24 February 2025, San Diego, CA, USA
ISBN 979-8-9919276-7-3
https://dx.doi.org/10.14722/futureg.2025.23099
www.ndss-symposium.org

potential vulnerabilities, including unauthorized access, policy manipulation, data breaches, and the risk that malicious rApps exploit RAN resources. These security challenges highlight the need for robust mechanisms to protect A1 and R1 communications. As mentioned in the O-RAN specifications, the A1 interface uses TLS 1.3 and JSON Web Tokens (JWT) for securing communications[4]. For data access uses the Role Based Access Control (RBAC) method. Although TLS and RBAC provide a foundational layer of security, they lack the granularity required to address advanced threats. Additionally, the Zero Trust Security study in 3GPP TR 33.894 [5] highlights that addressing compromised network functions relies on the specific implementation chosen by the operator.

In this context, we aim to integrate proactive security measures that can operate in a multi-vendor Non-RT RIC. Passive or reactive security measures are unsuitable for managing sensitive and critical telecommunication information. Unlike traditional reactive approaches, the salience of the proposed solution is that this is proactive on the Non-RT RIC itself, to prevent possible attacks on interfaces and Non-RT Framework functions. This proactive approach is highly necessary to build secure O-RAN compliant RIC applications for beyond 5G and 6G. Therefore, in summary, the key contributions of this work are as follows:

- Introducing an active secure communication approach to the RIC framework using the ABE variant.
- Identification of disruptions possible when one of the rApps is compromised under the multi-vendor Non-RT RIC.
- Integrating Attribute-Based Encryption to ensure the security of the interfaces (R1/A1) and other Non-RT RIC frameworks functions.

Attribute Based Encryption (ABE) emerges as a compelling solution, enabling policy-driven encryption and access control. This is in line with the Non-RT RIC functioning for the policy distribution to the Near-RT RIC. Among the two primary types of ABE, i.e., Key-Policy ABE (KPABE) and Ciphertext Policy ABE (CPABE) [6], [11], this work prefers CPABE as it facilitates more control over the service provider. ABE enables data encryption and decryption based on attributes (e.g., roles, locations, or functions) rather than specific identities, making it suitable for ORAN's dynamic, multi-tenant, and distributed architecture [7]. Simultaneously, the challenges encountered during the integration of ABE include:

A. Challenges in ABE Framework

- Performance overhead due to ABE's computation.
- Network overhead due to additional bytes transmitted.
- Real-time key distribution for dynamic networks.

The integration of ABE into the security of the non-RT RIC introduces considerable computational overhead due to its reliance on advanced cryptographic operations, such as pairing-based cryptography / elliptic curve cryptography, to enforce fine-grained access control [9], [11].

II. Background and Motivation

The risk associated with a malicious rApp (as shown in Fig. 2) and highlights the motivation for the proposed scheme. Communication among critical O-RAN components is vital.

A. Compromised rApp Creating Threats to Non-RT RIC

A compromised rApp with legitimate access to the Non-RT RIC leverages its permissions to execute malicious actions, threatening the security, availability, and integrity of the system. Here's how it unfolds:

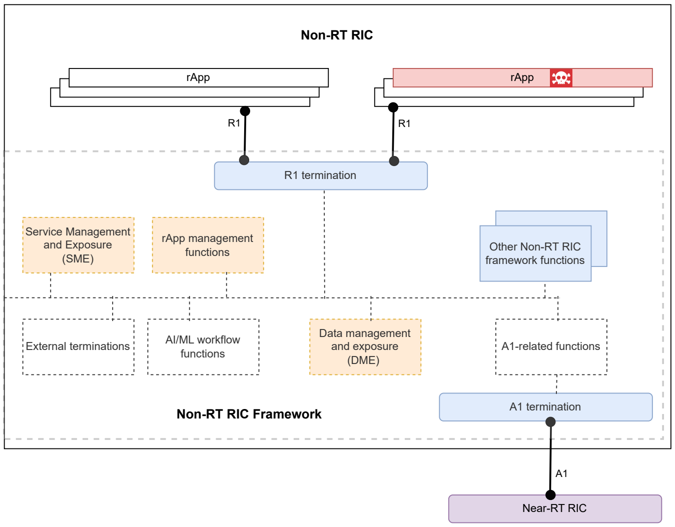
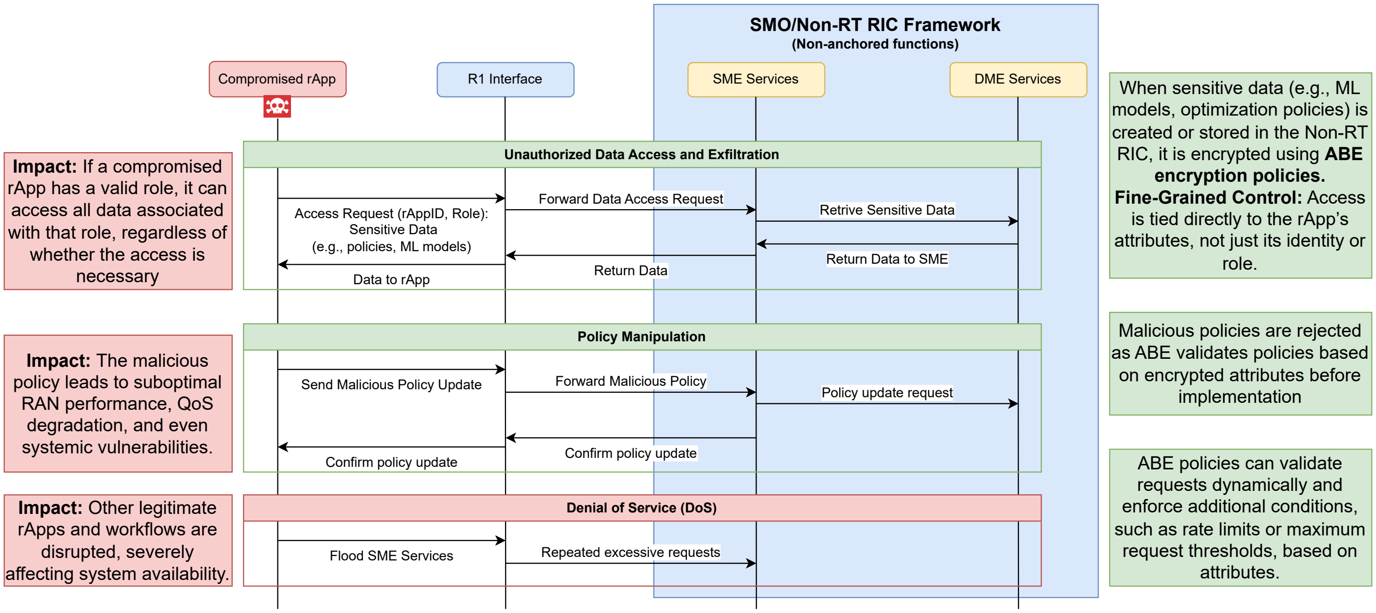


Fig. 2. Compromised rApp Creating Threats to Non-RT RIC

- **Unauthorized Data Access and Exfiltration**: A compromised rApp uses its legitimate access (validated by TLS and RBAC) to exfiltrate sensitive data, such as optimization policies, ML models, or subscriber insights.
- **Policy Manipulation:** The rApp injects or modifies the optimization policies in the Non-RT RIC, resulting in suboptimal RAN operations, degraded Quality of Service (QoS), or vulnerabilities in the network.
- **Denial of Service (DoS) on SME Services:** The malicious rApp floods the Service Management and Exposure (SME) services of the Non-RT RIC with excessive requests, disrupting legitimate rApp operations and hindering critical RAN optimization workflows.
- **Unauthorized Communication Across R1:** The rApp initiates unauthorized data sharing with other rApps or entities via the R1 interface, leading to data leaks or facilitating further compromise.

B. Motivation

The disaggregation and open interface features of ORAN expose more points of vulnerability, allowing attackers to exploit poorly secured interfaces or components, consequently increasing the attack surface [8], [10]. To address these challenges, it is essential to explore optimization techniques, such as lightweight ABE schemes [11], [14], [15], hardware acceleration, or hybrid encryption methods that combine ABE with



Impact: If a compromised rApp has a valid role, it can access all data associated with that role, regardless of whether the access is necessary

Impact: The malicious policy leads to suboptimal RAN performance, QoS degradation, and even systemic vulnerabilities.

Impact: Other legitimate rApps and workflows are disrupted, severely affecting system availability.

When sensitive data (e.g., ML models, optimization policies) is created or stored in the Non-RT RIC, it is encrypted using **ABE encryption policies. Fine-Grained Control:** Access is tied directly to the rApp's attributes, not just its identity or role.

Malicious policies are rejected as ABE validates policies based on encrypted attributes before implementation

ABE policies can validate requests dynamically and enforce additional conditions, such as rate limits or maximum request thresholds, based on attributes.

Fig. 3. Threats and ABE framework for Non-RT RIC

more computationally efficient approaches [16], [17] and pre-shared key schemes. Studies such as [12], [13] demonstrate the practicality of ABE in opportunistic and information-centric networks, inspiring our efforts to optimize encryption. The Non-RT RIC supports intelligent RAN optimization control loops with intervals exceeding one second [18].

- Mitigation Using ABE: Fine-Grained Access Control via Attributes:
  - Each rApp is assigned specific attributes, such as Policy_Access, Data_Read, or Model_Training, which dictate the scope of its operations.
  - Even if the rApp is compromised, its access is restricted to operations that match its attributes, preventing unauthorized data access or policy manipulation.

III. Threats in Non-RT RIC and Need for ABE Framework Solution

The comparison of TLS, RBAC, and ABE highlights why ABE is essential for robust security. Fig. 3 illustrates few possible threats in this case.

1) **Unauthorized Data Access and Exfiltration:** A compromised rApp uses its legitimate access credentials to exfiltrate sensitive data (e.g. ML models, optimization policies).
   - TLS secures the communication channel, but does not control what happens to the data once it reaches the rApp. A compromised rApp can misuse decrypted data.
   - mTLS ensures that only authenticated rApps communicate with Non-RT RIC, but once authenticated, it cannot restrict data misuse by a compromised rApp.
   - RBAC grants access based on roles, allowing the compromised rApp to access all data permissible for its role, even if not needed for its current operation.
   - **Fine-Grained Data Access:** Even if mTLS authenticates the rApp and RBAC permits access, ABE ensures that only rApps with the correct attributes (e.g., *Purpose=LoadBalancing, AccessLevel=High*) can decrypt and access specific data.
   - **Context-Aware Encryption:** Sensitive data are encrypted based on attributes. For instance, subscriber data may require *Region=India* and *Purpose=Analytics* for decryption, preventing unauthorized use even by authenticated rApps.
2) **Policy Manipulation:** A compromised rApp injects malicious optimization policies into the Non-RT RIC, causing degraded RAN performance or vulnerabilities.
   - TLS and mTLS ensure secure transmission of policies, but cannot validate the legitimacy of the policy content.
   - RBAC allows any rApp with the *PolicyManager* role to submit policies without validating the integrity or intent of the policy.
   - **Policy Validation via Attributes**: ABE ensures that policies are encrypted under attributes like *AuthorizedBy=Admin* and *PolicyType=QoSOptimization*. Malicious policies without these attributes are rejected during decryption.

   TLS protects the policy during transmission, and RBAC ensures that only authorized roles can submit policies. ABE goes further by ensuring that only valid encrypted policies with matching attributes are implemented.
3) **Denial of Service (DoS) Attacks:** A compromised rApp floods the R1 interface or SME services with excessive

requests, disrupting legitimate operations.

- TLS and mTLS ensure that requests come from authenticated rApps but do not limit their frequency.
- RBAC cannot enforce request limits or dynamically detect abnormal behavior.
- ABE policies can include rate-limiting attributes (e.g., *MaxRequests=100/sec*). Requests exceeding this limit are automatically rejected.

ABE adds a layer of defense by embedding rate limits and access frequency attributes, preventing excessive requests from disrupting operations.

4) **Unauthorized Communication Across R1:** A compromised rApp communicates with other rApps or external entities via the R1 interface, leading to data leaks or unauthorized data sharing.

- **No Post-Authentication Control:** mTLS and TLS ensure secure communication but do not prevent data sharing once the rApp is authenticated.
- **No Inter-rApp Restrictions:** RBAC does not control how data is shared between rApps or external entities after access is granted.
- **Controlled Data Sharing:** ABE enforces sharing restrictions by embedding attributes like SharingAllowed=False or RecipientRole=Analytics. Data cannot be shared without matching these attributes.

ABE embeds sharing restrictions directly into the data, ensuring that it remains protected even after access is granted.

A. Proposed ABE Solution

In the multi-vendor Non-RT RIC environment, ABE secures sensitive data and policies by enforcing fine-grained access control based on attributes (depicted in Fig. 4). Each piece of data is encrypted with a specific encryption policy, and only entities (e.g., rApps) with the required attribute set can decrypt it. Consider an example workflow as follows:

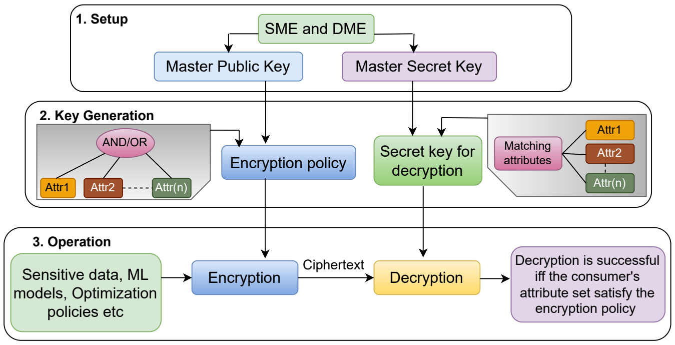


Fig. 4. Proposed ABE framework (ABElity)

1) **Encryption Policy:** A sensitive ML model is encrypted with the policy: *((Role=Analytics AND Region=IN) OR (Purpose=LoadBalancing AND AccessLevel=High))*.

2) **Attribute Set for rApps:**

- rApp A: *Role=Analytics, Region=IN, AccessLevel=Medium* → Can decrypt the ML model because it satisfies the first condition.
- rApp B: *Purpose=LoadBalancing, AccessLevel=Low* → Cannot decrypt because AccessLevel is insufficient.
- rApp C: *Purpose=LoadBalancing, AccessLevel=High* → Can decrypt because it satisfies the second condition.

3) **How It Works:**

- **Encryption:** The Non-RT RIC encrypts data or policies with an ABE encryption policy.
- **Decryption:** Only rApps with attribute sets that match the policy can decrypt and access the data.
- **Increased the security level:** Even if a malicious rApp has valid attributes for one operation, it cannot use them to access encrypted data for other purposes.

This ensures that only authorized rApp's specified role with the correct attributes can perform specific tasks, preventing unauthorized access, malicious policy manipulation, and sensitive data exfiltration.

IV. Experimental Setup

We plan to host the experimentation of the proposed solution using the O-RAN Software Community (OSC) framework [21]. Key generation and distribution will be managed within the SMO, while encryption and decryption will occur within the respective RIC frameworks as needed, as detailed in Section III-A. The experimental setup will include a Docker container hosting the Non-RT RIC and Near-RT RIC, with the A1 and R1 interfaces enabling communication. The interactions between the RICs will be monitored, and security-relevant attacks will be simulated to test the system's resilience. The proposed solution will be implemented to demonstrate its ability to counter these attacks and enhance security.

V. Conclusion

5G and Beyond networks will likely operate in an era where computational limitations will no longer be a barrier for brute-force encryption or even quantum computers may be viable. Recently, best to our knowledge, Google's Willow has achieved immense computational breakthrough [20]. This will only grow in the future, and we need quantum-safe solutions for communication. Quantum-resistant ABE ensures that critical data and policies are secure against future quantum adversaries. To make ABE quantum-resistant, cryptographic techniques that rely on lattice-based cryptography, code-based cryptography, or hash-based cryptography are used [19]. Another aspect we are planning to do is precompute parts of the quantum-resistant ABE operations to minimize computational overhead. After identifying the frequently used attributes, it is possible to pre-compute some of the ABE operations to reduce latency [14].

Acknowledgment

1. This work was supported by the project "Next Generation Wireless Research and Standardization on 5G and Beyond (RP04156G)", Ministry of Electronics and Information Technology, Government of India.

2. This work has been partially supported by the Dutch National Growth Fund 6G flagship project "Future Network Services".

References

[1] O-RAN Alliance, *A1 interface: General Aspects and Principles*, Technical Specification. O-RAN.WG2.A1GAP-R004-v04.00.

[2] O-RAN Alliance, *Non-RT RIC: Architecture*, Technical Specification. O-RAN.WG2.Non-RT-RIC-ARCH-R004-V06.00.

[3] F. Kaltenberger, T. Melodia, I. Ghauri, M. Polese, R. Knopp, T. T. Nguyen, S. Velumani, D. Villa, L. Bonati, R. Schmidt, S. Arora, M. Irazabal, N. Nikaein, *Driving Innovation in 6G Wireless Technologies: The OpenAirInterface Approach*, arXiv. 23(13), 2412.13295, 2024.

[4] O-RAN Alliance, *O-RAN Work Group 11 (Security Work Group) O-RAN Security*, Technical Specification. O-RAN.WG11.Security-Test-Specifications.0-R004-v08.00.

[5] 3GPP TR 33.894, *Study on applicability of the Zero Trust Security principles in mobile networks*, Technical Report. Release 18.

[6] J. Bethencourt, A. Sahai, and B. Waters, *Ciphertext-policy attribute-based encryption*, IEEE Symposium on Security and Privacy. SP '07, Berkeley, CA, USA, pp. 321–334, 2007.

[7] Z. Peng, C. Peng, Y. Tian, and H. Ding, *Bilateral Control for Secure Communication against Replay Attack in ORAN-based Vehicular Networks*, IEEE Transactions on Vehicular Technology (Early Access). pp. 1–14, 2024.

[8] M. S. Wani, M. Kretschmer, B. Schröder, A. Grebe, and M. Rademacher, *Open RAN: A Concise Overview*, IEEE Open Journal of the Communications Society (Early Access). 2024.

[9] F. Meng and L. Cheng, *TSR-ABE: Traceable and Server-Aided Revocable Ciphertext-Policy Attribute-Based Encryption under Static Assumptions*,IEEE Transactions on Information Forensics and Security (Early Access). 2024.

[10] H. Wen, P. Porras, V. Yegneswaran, A. Gehani, and Z. Lin, *5G-SPECTOR: An O-RAN Compliant Layer-3 Cellular Attack Detection Service*, In Proceedings of the 31st Annual Network and Distributed System Security Symposium, NDSS. Vol. 24, 2024.

[11] K. Sowjanya, M. Dasgupta, and S. Ray, *A lightweight key management scheme for key-escrow-free ECC-based CP-ABE for IoT healthcare systems*, Journal of Systems Architecture. Vol. 117, 102108, 2021.

[12] M. R. Asghar, A. Gehani, B. Crispo, and G. Russello, *PIDGIN: privacy-preserving interest and content sharing in opportunistic networks*, ASIA CCS '14: Proceedings of the 9th ACM symposium on Information, computer and communications security. pp 135 - 146, 2014.

[13] M. Raykova, H. Lakhani, H. Kazmi, and A. Gehani, *Decentralized Authorization and Privacy-Enhanced Routing for Information-Centric Networks*, ACSAC '15: Proceedings of the 31st Annual Computer Security Applications Conference . pp 31 - 40, 2015.

[14] Shruti, S. Rani, D. K. Sah, and G. Gianini, *Attribute-Based Encryption Schemes for Next Generation Wireless IoT Networks: A Comprehensive Survey*, Sensors. 23(13), pp. 5921, 2023.

[15] Y. Sun, X. Du, S. Niu, and S. Zhou, *A lightweight attribute-based signcryption scheme based on cloud-fog assisted in smart healthcare*, Plos one. 19(1), e0297002, 2024.

[16] C. Guo, B. Gong, M. Waqas, H. Alasmary, S. Tu, and S. Chen, *An efficient pairing-free ciphertext-policy attribute-based encryption scheme for Internet of Things*, Sensors (Basel, Switzerland). 24(1), 2024.

[17] M. Mahdavi, M. H. Tadayon, M. S. Haghighi, and Z. Ahmadian, *IoT-friendly, pre-computed and outsourced attribute based encryption*, Future Generation Computer Systems. Vol. 150, pp. 115–126, 2024.

[18] O-RAN Alliance, *Control, User and Synchronization Plane Specification-RAN Architecture Description*, Technical Specification. O-RAN.WG1.OAD-R003-V12.00.

[19] K. K. Singamaneni, G. Muhammad, and Z. Ali, *A Novel Quantum Hash-Based Attribute-Based Encryption Approach for Secure Data Integrity and Access Control in Mobile Edge Computing-Enabled Customer Behavior Analysis*, IEEE Access. Vol. 12, pp. 37378–37397, 2024.

[20] Google's Willow quantum chip, https://blog.google/technology/research/google-willow-quantum-chip/

[21] OSC, *implementation of NON-RT RIC, https://lf-o-ran-sc.atlassian.net/wiki/spaces/RICNR/overview*