2024 15th International Conference on Information and Communication Technology Convergence (ICTC) | 979-8-3503-6463-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICTC62082.2024.10826894

Roadmap for Integrating Open RAN and AI for Intrusion Detection Systems in 6G Networks

Love Allen Chijioke Ahakonye †, Cosmas Ifeanyi Nwakanma †, Dong-Seong Kim
IT Convergence Engineering, † ICT Convergence Research Center,
Kumoh National Institute of Technology Gumi, South Korea
(loveahakonye, cosmas.Ifeanyi, dskim)@kumoh.ac.kr

Abstract—**This work presents a roadmap for integrating Open Radio Access Networks (O-RAN) and Artificial Intelligence (AI) into 6G networks, focusing on intrusion and fault detection. O-RAN introduces flexibility in network design by enabling disaggregated and vendor-neutral components, but it also poses security challenges due to open interfaces and multi-vendor integration. This study proposes strategically deploying an intrusion detection system (IDS) within the O-RAN framework to enhance security. The IDS structure suggests specific placement of sensors at critical locations such as Near-Real-Time RAN Intelligent Controllers (RICs), Open Distributed Units (ODU), and Open Fronthaul interfaces, among others. This deployment is complemented by a federated learning approach for IDS model training, which ensures data privacy and resilience by keeping sensitive data local while improving model performance through aggregated updates. The paper emphasizes the importance of such a framework for the secure and efficient operation of 6G networks, addressing the challenges posed by the increasing complexity and potential vulnerabilities of O-RAN. The proposed roadmap is intended to guide stakeholders in mitigating risks and optimizing the integration of AI in future 6G networks.**

Index Terms—**AI, O-RAN, IDS, 6G**

I. Introduction

6G networks offer enhanced wireless communications [1], necessitating innovative architectures for various deployment strategies [2]. Open and disconnected frameworks are adjustable in optimization and choice of network functionalities and services [3]. The highlights and challenges of these configurations in radio access networks (RAN) have been examined [1]. Open-RAN (O-RAN) separates RAN components using open interface specifications and software virtualization [1], [3], [4], supporting vendor-neutral software-defined and hardware implementation through open interconnectivity and combined improved standards [4]. O-RAN enables virtualized, disaggregated, and open interface-connected RANs, introducing a new RAN blueprint, placement, and operations paradigm. O-RAN networks consist of multivendor, interoperable components optimized via a unified interface and data-oriented closed-loop administration, compelling robust protection of its architecture, interfaces, and workflows [3].

O-RAN integrates machine learning (ML) and artificial intelligence (AI) platforms to optimize performance, enhance user experience, enable predictive maintenance, and facilitate intrusion detection [5], [6]. These architectures offer benefits for 6G networks, including enhanced versatility in adopting and optimizing services and components [4]. This adaptability is crucial for meeting the varied needs of IoT networks. O-RAN exemplifies a structure that shifts network operations to the cloud, aiming for increased scalability and efficiency. Open and disaggregated architectures ease the 6G transition by enabling multi-vendor components' reusability and scalability, potentially ownership cost [1], [4].

Managing open interfaces and multiple vendors in O-RAN introduces security and integration obstacles. Critical innovations include the service management and orchestration components and RAN Intelligent Controller (RIC) [1], [4], [7]. Researchers propose using non-real-time applications (rApps) and near-real-time applications (xApps) to address these challenges [8]. rApps focus on RAN infrastructure management, while xApps handle use-case-specific logic and optimizations. xApps emphasizes application-specific deduction and optimizations, while rApps concentrate on controlling and managing the RAN configuration [9]. This approach lets operators choose the best third-party apps, enhancing network functionality and performance [1].

The 3GPP and O-RAN Alliance also provide blueprints and design principles to secure telecom functions and interfaces [1], [4]. Studies on understanding, threat modeling, and securing O-RAN interfaces have been underway [3], [10]–[12]. Considering strategic intrusion prediction and maintenance using intrusion detection mechanisms is imperative. However, additional security measures are needed to protect information, communication technology, and cloud systems. Following these ideal procedures are essential for sustaining secure, efficient and reliable networks while minimizing attack surfaces [1], [3], [4], [10], [11].

Given the findings and outlined vulnerabilities in [3], [10], [11], the best practice for IDS placement within the O-RAN architecture would ensure comprehensive monitoring and protection of critical components and interfaces. Key areas for IDS deployment should include Near-Real-Time RIC, open distributed and centralized unit, open fronthaul interface, xApp and rApp environment, management interfaces and user plane traffic [3], [10]. This study specifically presents the following contributions:

1) Analysis of O-RAN, its structure, applications, limitations and security in the 6G networks.
2) A conceptual framework for IDS placement within the O-RAN substructure.

3) Experimentation of the proposed concept with the publicly available Edge-IIoTset dataset.

Following Section I is Section II, reviewing existing studies in O-RAN security. Section III presents the conceptual framework proposed in this study. Section IV discusses the findings and experimentation and concludes in Section V.

II. Background and Related Studies

Holistically exploring the security of O-RAN, authors in [11] identified threats, discussed solutions, and demonstrated their effectiveness against cyber attacks on the advanced programmable O-RAN site, providing essential guidelines for researchers. Authors in [3] provide a detailed O-RAN tutorial, discussing its architecture, interfaces, and workflows. The study also explored its research challenges, including AI/ML integration, security, standardization, experimental research platforms, and future development directions. The O-RAN Alliance's Working Group 11 ensures secure-by-design specifications, addressing new security challenges due to an expanded threat surface [10]. The authors analyzed a vanilla O-RAN deployment, evaluated the endurance of various O-RAN interfaces under denial of service and performance degradation attacks, and identified mitigation mechanisms to improve future O-RAN network robustness.

Investigations on the effects of virtualization and software-based O-RAN systems focusing on the O-RAN ALLIANCE architecture and O-Cloud implementation using the software community base for O-RAN highlight potential vulnerabilities and misconfigurations in the Kubernetes infrastructure supporting the RIC [12]. They emphasized the need for integrated security evaluation methods, deployment hardening measures, and policy-based control to improve overall security. O-RAN RIC is one of the most demanding features [4], and studies suggest that security measures in O-RAN architectures command about 46% of the focus in the O-RAN community [1], [4], [8]. The authors present some Use Cases highlighting ML and deep learning models for predictive maintenance and network optimization. The realistic approach would be an open interface to integrate ML techniques [1], [4], [13].

Authors in [13] discussed vital technologies driving 6G development, including intent-based networking, Terahertz and quantum communication, blockchain, AI, smart devices, and communication without gadgets. Exploring these technologies' contribution to 6G addresses their potential, applicability, existing limitations, and prospective solutions. The consensus is that 6G will integrate AI as a core element, enabling ubiquitous AI services. This ”intelligence inclusion” will significantly influence 6G network architecture. In [5], the authors suggest a comprehensive system design for 6G, emphasizing the need for a separate data plane and an innovative, intelligent plane to manage AI workflows.

Traditional RAN solutions provide thoroughly tested, integrated software and hardware. O-RAN offers greater flexibility for operators in choosing components but introduces challenges in system integration and operational management [4]. O-RAN introduces challenges like security due to open interfaces, necessitating a zero-trust approach, and increased complexity in multivendor integration and operational management, where orchestration is crucial [4]. As an open, adaptive, and intelligent RAN architecture leveraging ML for network management, it is vulnerable to adversarial ML attacks. Edan et al. [14] systematically analyze adversarial ML threats in O-RAN, review potential attacks, illustrate an adversarial ML attack on a traffic pilot model, and propose countermeasures and a risk assessment methodology.

The open, adaptive, and intelligent RAN architecture heightens system vulnerability [10], [15]. This study proposes a conceptual framework to address security limitations in multivendor setups. An integrated agnostics IDS solution [16] should be implemented with sensors and monitoring points at critical locations within the O-RAN RIC. This IDS comprises a central monitoring and analysis unit aggregating data from all sensors, analyzing anomalies, and coordinating responses. Distributed IDS sensors at Open Distributed Unit (ODU), Open Centralized Unit (OCU), Open Fronthaul (OFH) interfaces, RIC nodes, management interfaces, and within xApp and rApp environments ensure comprehensive monitoring. Localizing IDS at these strategic points detects and mitigates unauthorized access, data breaches, conflicts, and other vulnerabilities, thus preserving the O-RAN network's integrity and security.

III. System Methodology

A. What is RAN?

RAN employs Radio linkage made up of Base stations (BS) to facilitate communication between the user equipment and the network center [3], [17]. Each BS has a radio unit for transmitting signals and a Baseband unit for managing resources and radio management. The primary function of the BS is radio resource control. The Core network manages access, mobility, and essential services like interconnectivity [17].

B. RAN Evolution

The last three decades have witnessed the evolution of RAN from monolithic, proprietary systems to disconnected setups utilizing commercial off-the-shelf hardware [17]. Base station types are discussed as follows:

1) Decentralized RAN (D-RAN): The radio and Baseband units are located within the cell site and operate locally. The Baseband is housed in a cool shelter, while the remote radio unit can be nearby or on the tower. Proprietary Baseband and remote radio units increase costs as user equipment and Base stations grow [17].
2) Centralized RAN (C-RAN): It centralizes Baseband units from multiple base stations to reduce site rental efforts. It also allows adding new remote radio units without new Baseband units, cost-effectively addressing traffic growth. It is limited by high fronthaul (FH) competence needs, vulnerability points and vendor lock-in, enabling suitability for urban areas [17].
3) Using the concepts of network function virtualization, virtualized RAN (vRAN) is an improved version of

C-RAN that uses commercial off-the-shelf servers in place of proprietary Baseband unit hardware. While the interface between Baseband and distant radio units is still proprietary, network services are operated on virtual machines or containers on commercial off-the-shelf hardware. Virtualizing Baseband pools allows resource sharing among sites, potentially reducing data processing needs by about 50%, with increased network complexity making resource sharing among radio nodes challenging [17].

C. Transition from vRAN to O-RAN

The shift from vRAN to O-RAN involved standardizing connections between RAN components and incorporating cloud-based elements from vRAN [17]. The primary changes include standardizing the open FH connectivity between remote radio and Baseband units and separating the Baseband Unit into distributed unit (DU) and central Unit (CU). Multi-vendor deployments of standardized interfaces enable operators to mix and match radio units, DUs, and CUs. commercial off-the-shelf-based software-defined radio replaces proprietary remote radio unit hardware. Decoupling Control and User Planes enhances the integration of data-driven intelligence for automated RAN management [17]. O-RAN fundamental architectural principles are as follows:

1) Virtualization: decouples hardware and software, allowing RAN functions to run on generic hardware platforms. It enables cost-efficient hardware, elastic resource scaling, and simplified orchestration, reducing operational costs [1], [3], [4].

2) Disaggregation: splits the base station into functional radio, distributed and central units (RU, DU, CU) and further divided into a control plane (CU-CP) and a user plane (U-UP), facilitating the deployment of diverse functionality across various locations and platforms [1], [3], [4].

3) Open interfaces: standardize component connections, enabling vendor interoperability. They also allow mixing and matching equipment based on performance, features, and costs. RIC embodies intelligence, optimizing RAN elements and resources. The non-RT RIC and near-R-T RIC host third-party ML/AI-powered applications for tasks like radio resource management and self-organizing network functionalities, enhancing network management and reducing costs [1], [3], [4].

D. Leading Groups in O-RAN

The O-RAN Alliance, established in 2018 from the merger of the C-RAN Alliance and the X-RAN forum, aims to promote openness and intelligence in RAN [4]. With over 300 members, it focuses on standardizing architecture and interfaces for O-RAN. It also develops open-source software and hardware and guides members in testing the interoperability of O-RAN solutions, primarily targeting 4G and 5G networks [4], [17].

The Telecom Infra Project, founded in 2016, seeks to provide universal internet access through a collaborative approach. It emphasizes deployments and execution of O-RAN, organizing plugfests and live field deployments, and training and implementing O-RAN solutions globally. Both organizations have a liaison agreement to enhance collaboration on interoperable O-RAN solutions through information exchange and validation activities [17].

E. System Design

This methodology outlines the strategic deployment of an agnostic IDS within the O-RAN architecture to ensure comprehensive monitoring and protection of critical components and interfaces.

F. Proposed O-RAN IDS Placement Strategy

1) Near-RT RIC: These IDS sensors monitor communications between the E2 nodes and near-RT RIC and interactions involving xApps. They detect and mitigate conflicts between the E2 nodes and near-RT RIC and monitor xApp behavior.

2) Open Distributed (ODU) and Open Centralized Units (OCU): ODU and OCU IDS sensors monitor access attempts and communication traffic to and from ODU and OCU to prevent unauthorized access and protect S-Plane and C-Plane communications.

3) Open Fronthaul Interface (OFH): These IDS sensors inspect traffic passing through the OFH interface to protect C-Plane and S-Plane communications between the open radio unit and ODU.

4) xApp and rApp Environment: These IDS sensors monitor the execution and data access patterns of xApps and rApps within non-RT RIC and near-RT RIC environments. It will enable the prevention of conflicts and unauthorized access to subscriber data.

5) Management Interfaces: These IDS sensors monitor management interfaces for configuration changes and access attempts against unauthorized access and DoS attacks.

6) User Plane (U-Plane) Traffic: The IDS sensors monitor control messages and data traffic within the U-Plane to detect and prevent malicious control messages and unauthorized data access.

7) Integrated IDS Framework: The integrated IDS solution should comprise a central monitoring and analysis unit to address these vulnerabilities effectively. This unit will enable data aggregation from all IDS sensors, analyze them for anomalies, and coordinate responses. A centralized location is vital for comprehensive data analysis and threat response coordination. Lastly, the distributed IDS sensors at each critical location ensure prompt threat detection by providing localized monitoring at strategic points within ODU, OCU, OFH interfaces, RIC nodes, management interfaces, and xApp/rApp environments.

8) Process Workflow: The process workflow involves collecting data using IDS sensors from various points within the O-RAN framework. The central monitoring and analysis unit aggregates the collected data. Defined security rules and ML models enable the identification of anomalies, which trigger alerts to the network. The central unit coordinates responses by blocking malicious traffic or reconfiguring components. Fig. 1

overviews the proposed IDS placement strategy and integration of O-RAN and AI in 6G networks.

Recent studies highlight that new O-RAN elements like non-RT RIC, SMO and near-RT RIC offer new capabilities and potential vulnerabilities [10]. The architecture has open interfaces A1, E2, O1, O2, and OFH, which make it prone to attacks. The O-RAN 7.2x standard [15] identifies threats from these functions and interfaces in split 5G base stations [18]. Disaggregation expands trust chains, increasing the attack surface and the network function virtualization, enhancing flexibility and programmability, and heightening security risks. Open-source code from unverified repositories exposes components to known exploits; additionally, immature or inadequate O-RAN implementations may introduce further security threats [10].

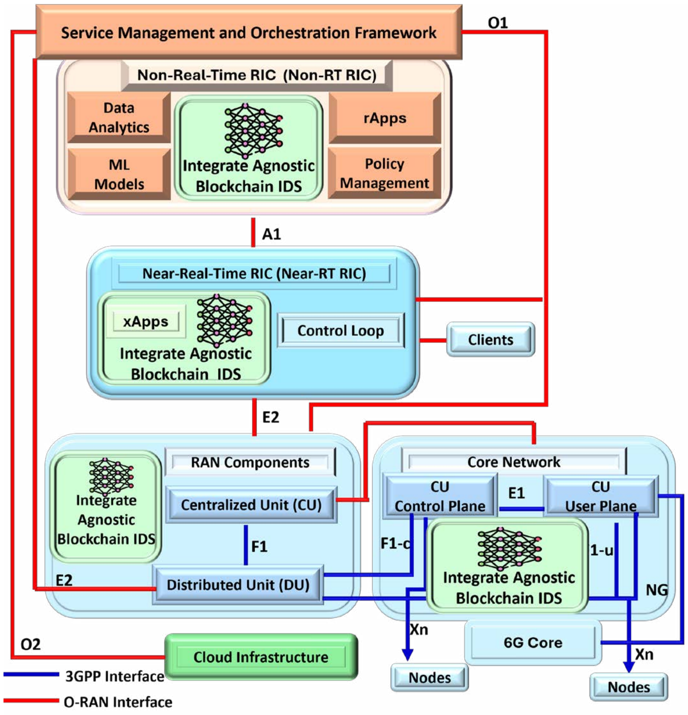

Fig. 1: Proposed O-RAN IDS Placement Strategy

G. Centralized Versus Federated Model Training for O-RAN IDS Framework

In centralized model training, data from various sensors and monitoring points within the O-RAN architecture is aggregated in a central repository for ML model training. This large, centralized dataset enhances model performance and accuracy by capturing diverse scenarios and anomalies. Centralized training simplifies ML model management, updates, and improvements using high-performance central servers, which can be more efficient than distributed resources [19]. However, this method raises data privacy and security concerns due to transferring and storing sensitive information in a central location. As data volume increases, centralized storage and processing can become bottlenecks, leading to performance issues and creating a single point of failure, a critical risk in large-scale deployments.

The ML model in a federated model learning is trained across IDS sensors at various points in the O-RAN architecture without transferring raw data to a central repository. Each device trains the model locally and shares only model updates with a central server, aggregating these updates to enhance the global model. This approach minimizes privacy concerns and complies with data protection regulations by keeping sensitive data local. It scales better with more devices, as the central server aggregates only model updates, not raw data, and is resilient against single points of failure. However, federated learning is more complex, requiring robust communication protocols and synchronization mechanisms. Local devices need adequate computational resources to train the model, which may only sometimes be available. Variability in data distribution and quality across devices can affect the consistency and performance of the global model.

H. Suggested Best Practice for IDS Model Training Scheme in O-RAN

Considering the specifics of the O-RAN structure and the objectives of the IDS placement strategy, blockchain-based federated model training is suggested as the best practice. It ensures that sensitive data collected by IDS sensors remains local, mitigating privacy and security concerns. As the number of IDS sensors and the volume of data grows, it can scale more efficiently without the need for a massive centralized data repository and enhance the resilience of the IDS framework, avoiding single points of failure and ensuring continuous protection even if some sensors go offline. Algorithm 1 summarizes O-RAN architecture's proposed federated learning-based IDS.

IV. Experimentation and Result Discussion

A. Dataset Description

The study validated the concepts using the Edge-IIoTset [1] dataset, comprising 62 predictors, 15 classifications, and 157,800 observations in Edge-IIoTset. This dataset was created for academic purposes and features diverse network attack types in IoT and IIoT scenarios. It covers metadata, eventdata, device identifiers, communication protocols, regular traffic, and common IoT cyberattacks, including DoS, unauthorized commands, man-in-the-middle (MiTM), reconnaissance, command injection, and backdoor attacks. Comprising specific sensor data featuring properties like source and destination IP addresses and ports, protocols, packet length, flow time, and statistics, it was chosen for its relevance, comprehensively depicting communication within a highly vulnerable heterogeneous IIoT network. The experimentation environment was Visual Studio Code, Python 3.6.13 on an Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz system with 8GB RAM running Windows 11.

[1] https://ieee-dataport.org/documents/edge-iiotset-new-comprehensive-realistic-cyber-security-dataset-iot-and-iiot-applications

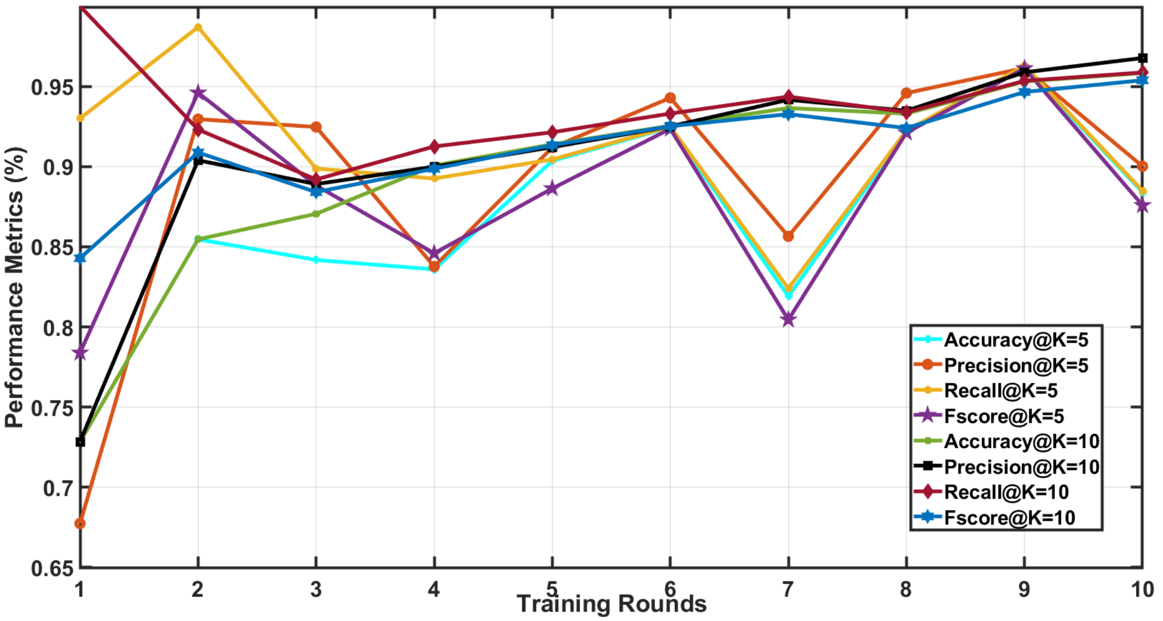

Fig. 2: Visualization plot illustrating the performance of the proposed IDS placement concept in the 6G O-RAN architecture

Algorithm 1 Federated Training IDS Placement

```
Function FEDERATEDTRAINING():
    global_model ← INITIALIZE_MODEL()
    num_rounds ← 10
    num_devices ← COUNT_IDS_SENSORS()
for round ← 1 to num_rounds do
        model_updates ← []
    for device ← 1 to num_devices do
            local_model ← TRAIN_LOCAL_MODEL(global_model, device_data[device])
            model_updates.APPEND(local_model.GET_GRADIENTS())
    end for
        global_model ← AGGREGATE_UPDATES(global_model, model_updates)
end for
    return global_model

Function MAIN():
    DEFINE_IDS_PLACEMENT()
    DEFINE_IDS_FRAMEWORK()
    trained_model ← FEDERATEDTRAINING()
    IDS_WORKFLOW(trained_model)

MAIN()
```

B. Performance Evaluation of the Experimentation of the Proposed Concept

The proposed framework was experimented on and evaluated on a federated learning architecture of two set-ups comprising five (5) and ten (10) clients for 10 rounds. Fig. 2 shows the accuracy graph comparison of the different clients, with an increasing trend with more clients, maintaining above 90% accuracy. Contrarily, the training with 5 clients exhibited instability over 10 training rounds and a plunge to 80% accuracy. It suggests the applicability and suitability of the proposed concept in the O-RAN architecture with diverse third-party connectivity for intrusion detection.

TABLE I: Comparison of distributed and centralized training performance of 5 and 10 clients over 10 rounds

Metrics	5 Clients		10 Clients	
	Distributed	Centralized	Distributed	Centralized
Accuracy (%)	88.5	88.4	**95.8**	**95.8**
Precision (%)	90.0	90.0	**96.8**	**96.8**
Recall (%)	88.5	88.5	**95.9**	**95.9**
F1-score (%)	87.6	87.6	**95.4**	**95.4**
loss #	0.702	0.711	**0.108**	**0.107**
Time (ms)	61,000	61,000	**52,000**	**52,000**

Experimentation results suggest the proposed concept is applicable and suitable for intrusion detection in the O-RAN architecture with diverse third-party connectivity. This is demonstrated by increasing the number of clients from 5 to 10, which significantly enhances the performance of federated learning, with improvements across loss, accuracy, F1 score, precision, and recall as in Table I. The model exhibits more consistent and stable learning with 10 clients, likely due to better resource utilization and diversity in the data provided by more clients. The evaluation time is also more efficient with 10 clients (52,000 ms), further supporting the benefits of a larger client pool in 6G O-RAN architecture with distributed scenarios.

V. Conclusions

The results from the federated learning experimentation suggest that integrating AI-IDS into the 6G O-RAN architecture is promising. It shows scalability with improved model performance as the number of clients increases. The consistent evaluation time of 10 clients indicates effective management of increased client participation without increased overhead. The minimal loss values with a client base indicate a better generalization across diverse data sources, which is essential for 6G O-RAN with varied and non-uniform traffic patterns and threats. The close alignment between the performance of distributed and centralized models suggests that the proposed approach can maintain high detection accuracy without the need to centralize data, which is particularly advantageous in 6G O-RAN, where data privacy and security are paramount, and edge-based processing is preferred. Our findings on the conceptual idea support the viability of a distributed framework as a robust, scalable, and privacy-preserving solution for IDS in 6G O-RAN, offering enhanced performance, efficiency, and adaptability. This decentralized approach ensures data privacy, aligns with the edge-centric nature of 6G, and can handle the diverse and dynamic conditions expected in future networks. Our future direction is to establish blockchain integration for secure and improved intrusion detection accuracy with the least evaluation time.

Acknowledgment

This research was supported by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003) (50%) and by MSIT under the Innovative Human Resource Development for Local Intellectualization support program (IITP-2024-2020-0-01612) (50%) supervised by the IITP.

References

[1] Erkens, H and Mildh, G. and Hoymann, C. and Summer, R. and Camps Mer, D. and Garcia, G. and Municio, E. and Moerman, Ingrid and Gallard, C. and Garcia Saavedra, A. and Hassan, M.S. and Wang, Y. and Akdogan, F. and Bey, T. and di Giglio, A. and Gianola, P. and Chassaigne, A. and Rodriguez, B.G. and Vazquez, M. and Lopez, R. and Martinez, M. and Tao, C. and Pyrivolakys, O. and Barani, B. and Kaloxylos, A. and Garcia, A., "6G Smart Networks and Services Industry Association (6G-IA)," p. 43, 2024. [Online]. Available: http://hdl.handle.net/1854/LU-01HXV50HSR82XE7H5W325CQJW3

[2] J. Hoydis, F. A. Aoudia, A. Valcarce, and H. Viswanathan, "Toward A 6G AI-Native Air Interface," *IEEE Communications Magazine*, vol. 59, no. 5, pp. 76–81, 2021.

[3] 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.

[4] A. J. Choi, "AI-Native Open RAN for 6G," July, 2023. [Online]. Available: https://www.gov.uk/government/publications/uk-open-ran-principles/open-ran-principles

[5] J. Wu, R. Li, X. An, C. Peng, Z. Liu, J. Crowcroft, and H. Zhang, "Toward Native Artificial Intelligence in 6G Networks: System Design, Architectures, and Paradigms," *arXiv preprint arXiv:2103.02823*, 2021.

[6] O. A. Karachalios, A. Zafeiropoulos, K. Kontovasilis, and S. Papavassiliou, "Distributed Machine Learning and Native AI Enablers for End-to-End Resources Management in 6G," *Electronics*, vol. 12, no. 18, p. 3761, 2023.

[7] C. Li, W. Hua, A. Ming, and S. Shaohui, "AI-native User-Centric Network for 6G," in *2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, 2022, pp. 494–499.

[8] M. Dryjański, Ł. Kułacz, and A. Kliks, "Toward Modular and Flexible Open RAN Implementations in 6G Networks: Traffic Steering Use Case and O-RAN xApps," *Sensors*, vol. 21, no. 24, p. 8173, 2021.

[9] D. Dalai, S. Babu, and M. BS, "Satellite-6G Network Integration Roadmap on Reference Architectures," *Authorea Preprints*, August 2022. [Online]. Available: http://dx.doi.org/10.36227/techrxiv.20624685.v1

[10] P. Baguer, G. M. Yilma, E. Municio, G. Garcia-Aviles, A. Garcia-Saavedra, M. Liebsch, and X. Costa-Pérez, "Attacking O-RAN Interfaces: Threat Modeling, Analysis and Practical Experimentation," *IEEE Open Journal of the Communications Society*, pp. 1–1, 2024.

[11] J. Groen, S. D'Oro, U. Demir, L. Bonati, D. Villa, M. Polese, T. Melodia, and K. Chowdhury, "Securing O-RAN Open Interfaces," *IEEE Transactions on Mobile Computing*, pp. 1–13, 2024.

[12] F. Klement, A. Brighente, M. Polese, M. Conti, and S. Katzenbeisser, "Securing the Open RAN Infrastructure: Exploring Vulnerabilities in Kubernetes Deployments," *arXiv preprint arXiv:2405.01888*, 2024.

[13] C. De Alwis, P. Kumar, Q.-V. Pham, K. Dev, A. Kalla, M. Liyanage, and W.-J. Hwang, "Towards 6G: Key Technological Directions," *ICT Express*, vol. 9, no. 4, pp. 525–533, 2023.

[14] E. Habler, R. Bitton, D. Avraham, D. Mimran, E. Klevansky, O. Brodt, H. Lehmann, Y. Elovici, and A. Shabtai, "Adversarial Machine Learning Threat Analysis and Remediation in Open Radio Access Network (O-RAN)," *arXiv preprint arXiv:2201.06093*, 2022.

[15] L. M. P. Larsen, A. Checko, and H. L. Christiansen, "A Survey of the Functional Splits Proposed for 5G Mobile Crosshaul Networks," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 146–172, 2019.

[16] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Agnostic CH-DT Technique for SCADA Network High-Dimensional Data-Aware Intrusion Detection System," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10 344–10 356, 2023. [Online]. Available: https://doi.org/10.1109/JIOT.2023.3237797

[17] M. S. Wani, M. Kretschmer, B. Schröder, A. Grebe, and M. Rademacher, "Open RAN: A Concise Overview," *IEEE Open Journal of the Communications Society*, pp. 1–1, 2024.

[18] D. S. Kim, J. M. Lee, C. I. Nwakanma, and H. Trang-Dang, "Campus-Based Test-Bed Implementation of 5G+ Networks at the 28 GHz Band: Challenges and Opportunities," *Journal of Korean Institute of Communications and Information Sciences*, vol. 48, no. 8, pp. 1031–1048, 2023.

[19] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Trees Bootstrap Aggregation for Detection and Characterization of IoT-SCADA Network Traffic," *IEEE Transactions on Industrial Informatics*, pp. 1–12, 2023. [Online]. Available: https://doi.org/10.1109/TII.2023.3333438