Joint Blockchain and Collaborative Learning for Novel Zero-Trust Massive IoT in 6G Networks

Ahmad Zainudin[*†], Revin Naufal Alief[§], Made Adi Paramartha Putra[§], Dong-Seong Kim[§], and Jae-Min Lee[§]
[*]Department of Electronic Engineering, Kumoh National Institute of Technology, Gumi, South Korea
[§]Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea
[†]Department of Electrical Engineering, Politeknik Elektronika Negeri Surabaya, Surabaya, Indonesia
(zai*, revinnaufal, mdparamartha95, dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—This study proposes a joint blockchain and collaborative learning mechanism to address those issues through a novel zero-trust massive IoT architecture development. The intelligence distributed network management and security (DNMS), decentralized authentication and access control (DAAC), and verifiable and data integrity (VDI) modules are employed to provide a zero-trust mechanism and enhance security schemes in 6G networks. A proof of concept validates the system's efficiency, indicating the proposed system's superior performance compared to state-of-the-art approaches.**

***Index Terms*—Zero-trust architecture (ZTA), Collaborative attack detection, Blockchain-based decentralized authentication, Verifiable and tamper-resistant model exchange, Massive IoT, and 6G network**

I. Introduction

The heterogeneous connectivity of the massive Internet of Things (IoT) with extreme data rates in 6G networks offers significant advantages by generating vast amounts of real-time data for various intelligent IoT services. Nevertheless, the heterogeneous protocol connections of massive IoT devices and the significant increase in sensed data from cyber-physical systems (CPS) in the 6G network render them vulnerable to sophisticated cyber attacks [1]. Conventional security architectures assume that once devices are authenticated within a network, they're implicitly trusted, allowing unrestricted access and data exchange, which can lead to security threats [2]. Furthermore, this approach is considered a single-network solution, unsuitable for next-generation networks (NGNs). Zero-trust architecture (ZTA) is a new paradigm that assumes all entities involved in the massive network are untrustworthy unless they are continuously authorized or confirmed to be secure [3]. However, adopting ZTA in a massive IoT 6G network poses technical implementation challenges to provide efficient, robust, and scalable security schemes.

A security framework using artificial intelligence (AI) and zero-trust techniques was deployed to enable the security scheme of the 6G network. This system utilizes honeypots, monitoring, and decision-making agents to detect and mitigate suspected attacks [4]. However, this approach lacks an authentication mechanism to verify the trustworthiness of the entities within the network. Furthermore, a blockchain-based data-sharing protocol was implemented in a zero-trust environment, enabling a decentralized authentication scheme [5]. Nevertheless, this framework does not consider a mechanism to guarantee the integrity of the shared data information. Considering the necessity of an enhanced security mechanism that provides a ZTA for massive IoT in 6G networks, this study proposes potential contributions: **(i)** We proposed a joint blockchain and collaborative learning to deploy the ZTA framework in the 6G networks, which consists of distributed network management and security (DNMS), decentralized authentication and access control (DAAC), and verifiable and data integrity (VDI) modules. **(ii)** We deployed the DNMS module using integrated blockchain-federated learning (BFL) to provide intelligence threat detection and mitigation.

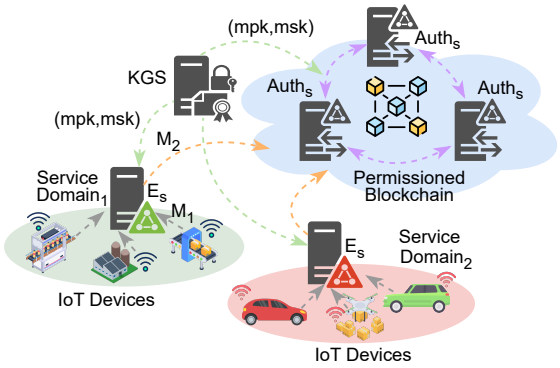

Fig. 1. Blockchain-based cross-domain anonymous batch authentication (BCA-BAuth)

II. Proposed Zero-Trust Architecture (ZTA) for Massive IoT in 6G Network

Blockchain provides decentralized authentication and avoids single-point-of-failure attacks in centralized authentication, such as public key infrastructure (PKI) with a certificate authority (CA) [7]. The proposed BCA-BAuth scheme is presented in Figure 1 and consists of IoT devices d, edge server E_s, authentication server $Auth_s$, and key generator server KGS. In the initialization step, KGS chooses an elliptic curve $G(F_p)$ $y^2 = x^3 + ax + b\,(mod\,p)$, p is prime number and the element of the $G(F_p)$ are $\{0, 1, 2, .., p-1\}$. Subsequently, KGS defines the hash function $\mathbb{H} : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ and shares the global parameter with the blockchain. The KGS randomly selects the master private key msk, and the master public key is obtained as $mpk = msk.\,P$. The KGS distributes the

TABLE I
COMPARISON OF EXISTING FL-BASED DECENTRALIZED THREAT DETECTION MODELS FOR IOT NETWORKS

Method	Accuracy	Precision	Recall	F1-Score	Loss	AUC Score	Trainable Parameters	Model Size	MFLOPS
CNN	94.74%	94.89%	94.19%	94.09%	0.1284	0.9498	15,128	60.52 KB	0.0302
DNN	95.23%	95.66%	95.62%	95.41%	0.0583	0.9539	18,368	63.25 KB	0.0319
LSTM	93.16%	92.89%	93.22%	93.14%	0.1605	0.9453	86,368	363.85 KB	0.1683
CNN-BiLSTM [2]	95.32%	95.64%	95.13%	94.54%	0.0504	0.9755	21,194	74.65 KB	0.0383
IDSFedNet [6]	97.28%	97.32%	97.16%	96.95%	0.0482	0.9738	14,627	58.85 KB	0.0296
Proposed	**98.78%**	**98.64%**	**98.72%**	**98.63%**	**0.0351**	**0.9884**	**5,523**	**16.68 KB**	**0.0082**

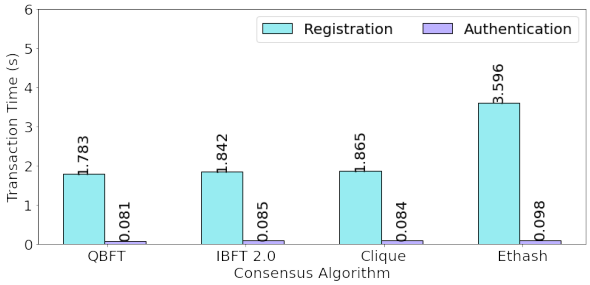

Fig. 2. Computation time of decentralized authentication performance

private and public keys to the IoT devices for each domain using a secure communication channel in the registration step. If the IoT device in service domain 1 d_i^1 wants to access the device in service domain 2 d_j^2, the d_i^1 sends a request message to E_s $M_1 = \left\{ID_{d_j^2}, request\right\}$. The E_s verify and create the authentication parameters of the IoT device d_i^1. Subsequently, sign the parameters message using their private key $M_2 = Sign\left(SK_{E_s}, \left(\{PID, PK_c\}, ID_{d_2^j}\right)\right)$ and forwards to $Auth_s$, where PID, PK, and SK denote pseudonyms, private, and public keys, respectively. Then, $Auth_s$ verifies the M_2 using E_s's public key, calculate $\alpha_p = \mathbb{H}\left(PID_r \,||\, PK_{cp} \,||\, ID_{d_j^2}\right)$ and store α_p to the blockhain. For further cross-domain authentication, just access through the smart contract to query α_p is available in the blockchain. This decentralized authentication is used to ensure the entity in the network is trusted before conducting the training task to develop a decentralized IDS model by utilizing IoT devices as the FL clients. The conventional FL technique faces several challenges, including using a central-centric aggregation mechanism susceptible to a single point of failure (SPoF) attack. Furthermore, the malicious clients can inject false data during the aggregation process, affecting the model performance. Therefore, the DNMS is integrated with the VDI module by leveraging the blockchain network and IPFS

III. EXPERIMENTAL RESULTS AND DISCUSSION

Table I presents the comparative analysis between the proposed model and existing collaborative IDS for IoT networks. This evaluation compares various techniques, including CNN, DNN, LSTM, CNN-BiLSTM [2], and IDSFedNet [6]. CNN-BiLSTM model performed an accuracy of 95.32% with $21,194$ trainable parameters, while the IDSFedNet model achieved 97.28% accuracy with $14,627$ trainable parameters. Based on this comparison, the proposed model outperforms these benchmarks, achieving an accuracy of 98.78% with a lightweight model architecture. This model has $5,523$ trainable parameters, a model size of 16.68 KB, and computes MFLOPs of 0.0082. Figure 2 presents the performance of the proposed blockchain-based decentralized authentication BCA-BAuth. Based on the evaluation results, superior performance is achieved when using QBFT consensus. The transaction time of the *Registration()* function is 1.783 ms, and for *Authentication()* function is 0.081 ms.

IV. CONCLUSION

This paper integrates blockchain and collaborative learning to provide a novel zero-trust architecture (ZTA) in massive IoT 6G networks. Based on the evaluation results, the proposed system can provide a robust and efficient ZTA environment. For future work, consider integrating a more scalable hybrid blockchain with generative AI to deploy a zero-trust mechanism.

ACKNOWLEDGMENT

This work was partly supported by the Innovative Human Resource Development for Local Intellectualization program through the Institute of IITP grant funded by the Korea government(MSIT) (IITP-2024-2020-0-01612, 50%) and by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003, 50%).

REFERENCES

[1] B. D. Son, N. T. Hoa, T. Van Chien, W. Khalid, M. A. Ferrag, W. Choi, and M. Debbah, "Adversarial Attacks and Defenses in 6G Network-Assisted IoT Systems," *IEEE Internet of Things Journal*, 2024.

[2] E. C. Nkoro, J. N. Njoku, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Zero-Trust Marine Cyberdefense for IoT-Based Communications: An Explainable Approach," *Electronics*, vol. 13, no. 2, p. 276, 2024.

[3] X. Chen, W. Feng, N. Ge, and Y. Zhang, "Zero Trust Architecture for 6G Security," *IEEE Network, 2023*, 2023.

[4] H. Sedjelmaci, K. Tourki, and N. Ansari, "Enabling 6G Security: The Synergy of Zero Trust Architecture and Artificial Intelligence," *IEEE Network*, 2023.

[5] Y. Liu, X. Hao, W. Ren, R. Xiong, T. Zhu, K.-K. R. Choo, and G. Min, "A Blockchain-based Decentralized, Fair and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things," *IEEE Transactions on Computers*, vol. 72, no. 2, pp. 501–512, 2022.

[6] A. Zainudin, R. Akter, D.-S. Kim, and J.-M. Lee, "Federated Learning Inspired Low-Complexity Intrusion Detection and Classification Technique for SDN-Based Industrial CPS," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 2442–2459, 2023.

[7] A. Zainudin, M. A. P. Putra, R. N. Alief, R. Akter, D.-S. Kim, and J.-M. Lee, "Blockchain-Inspired Collaborative Cyber-Attacks Detection for Securing Metaverse," *IEEE Internet of Things Journal*, 2024.