Blockchain-based Novel Collaborative Threat Detection in Industrial Cyber-Physical Systems

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 an enhanced security scheme for industrial CPS by utilizing integrated blockchain, hierarchical federated learning (HFL), and aggregated signature techniques to develop a trusted and verifiable collaborative threat detection (CTD) framework. A verifiable off-on-chain aggregation mechanism is implemented to provide secure and tamper-resistant model aggregation with minimum transaction time, meeting the requirements of industrial services. Additionally, an efficient signature method is employed during the aggregation process to ensure the confidentiality and integrity of the model exchange.**

***Index Terms*—collaborative threat detection (CTD), verifiable off-on-chain aggregation, efficient signature, industrial cyber-physical systems (CPS)**

I. Introduction

Industrial CPS facilitates enhanced industrial processes with heterogeneous connectivity capabilities supported by emerging technologies such as machine learning (ML), blockchain, digital tins (DT), massive Internet of Things (IoT), and future wireless networks. However, this capability is vulnerable to sophisticated attacks and adversarial threats [1]. ML and deep learning (DL)-based intrusion detection system (IDS) methods have been deployed to secure IIoT networks by exploiting centralized learning (CL) abilities, preventing and mitigating cyber threats [2]. The decentralized paradigm shifts training to the edge by utilizing the federated learning (FL) technique to develop a collaborative threat detection (CTD) and address limitations in CL scenarios, such as lack of data privacy, high communication overhead, and issues with high power usage [3]. Nevertheless, conventional FL techniques often use a central-centric aggregation mechanism that suffers from a single point of failure (SPoF) and requires more communication resources. Moreover, poisoning attacks can tamper and inject false data during aggregation, affecting the reliability of the aggregated model [4].

Employing blockchain in the FL environment provides transparency, integrity, traceability, and trustworthiness during training. Blockchain allows for a trusted decentralized mode without needing credit endorsement from third parties that is required in industrial applications [5]. However, the main challenges of blockchain-FL integration are associated with scalability, leading to high latency and decreased throughput, which causes the system to fail to meet the real-time and low-latency requirements in industrial services [6]. Considering the necessity of an improved security scheme that prioritizes privacy, efficiency, low latency, and trust in detecting cyber attacks for industrial CPS, this study proposes potential contributions: **(i)** We proposed a blockchain-based collaborative network intrusion detection system using hierarchical federated learning (HFL) to provide a communication-efficient decentralized cyber threat detection for industrial CPS. Several trusted FL client clusters were created according to industrial service, which the cluster coordinator handled for local training and generated a cluster global model. **(ii)** We implemented a verifiable off-on-chain aggregation technique for each cluster to provide a secure and anti-tampering model aggregation with minimum transaction time. A lightweight and robust digital signature was employed to verify the model parameters exchange during the aggregation process.

II. Proposed Efficient Blockchain-based Collaborative Threat Detection

To develop the verifiable off-on-chain module, we utilize IPFS as the trusted off-chain storage and RSA signature algorithm to verify model exchange between edge devices, cluster coordinator, and validator. First, the C_{main} share the initial weight of the model to the industrial edge devices FL client e_i through their cluster coordinator. At the first round r, where $r \in R = \{1, 2, 3, .., R\}$, each client executes the received initial weight to perform local training using their raw data and generate the local model, denoted as the $\omega_{n,r}^{local}$. Subsequently, store the updated local model on the client's IPFS and generate a content identifier (CID) for the local model $\mathrm{CID}_{n,r}^{local}$. CID is a label used to access the material in the IPFS. The FL clients produce a 1024 key-pair and sign the $\mathrm{CID}_{n,r}^{local}$ utilize RSA private key $\{p, d\}$, where p and d are typically big integers. In sequence, calculate their local model hash h_{local} using SHA-512 and encrypt h_{local} to execute the signature $sign_{local}^{\mathrm{CID}}$.

The edge devices share the signed CID local model $\mathrm{CID}_{n,r}^{local,signed}$, original $\mathrm{CID}_{n,r}^{local}$, and private key to the cluster coordinator. The verified $\mathrm{CID}_{n,r}^{local}$ that aggregated from all clients and fog servers are calculated to generate an aggregated local model using the FedAverage aggregation algorithm, store it on the IPFS cluster coordinator, and generate aggregated local model CID $\mathrm{CID}_{k,r}^{agg\_local}$. Subsequently, the cluster coordinator calculates the aggregated local model hash

TABLE I
COMPARISON OF EXISTING COLLABORATIVE THREAT DETECTION TECHNIQUES FOR BLOCKCHAIN-BASED INDUSTRIAL CPS

Method	Accuracy	Precision	Recall	F1-Score	Loss	AUC Score	Trainable Parameters	Model Size	MFLOPS
Multi-MLP	97.86%	86.85%	85.35%	85.84%	0.0726	0.9786	63,642	248.60 KB	0.1254
IDSFedNet [7]	97.87%	86.41%	85.66%	85.71%	0.0631	0.9788	13,928	54.41 KB	0.0267
MiTFed [8]	97.88%	86.74%	85.03%	85.68%	0.0619	0.9787	45,394	177.32 KB	0.0901
Proposed	**98.59%**	**88.01%**	**86.41%**	**86.91%**	**0.0451**	**0.9860**	**4,042**	**15.79 KB**	**0.0074**

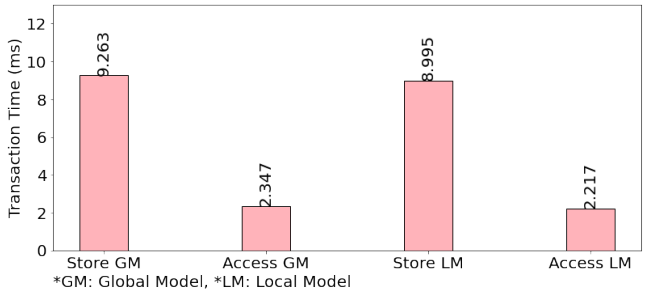

Fig. 1. Transaction time of IPFS-based off-chain aggregation (store GM, access GM, store LM, and access LM)

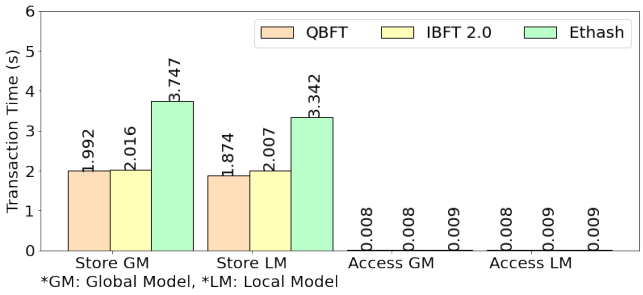

Fig. 2. Transaction time of storing aggregated global model for on-chain aggregation with different consensus algorithms

h_{agg_local} using the same RSA configuration with edge devices to enforce the signature $sign^{\text{CID}}_{agg\_local}$. The validator collects the aggregated local models from all cluster coordinators to calculate the aggregated global model and store the blockchain network.

III. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed model was developed using the CNN model while utilizing the grouped and factorized configuration to achieve an efficient model structure. Table I presents the comparison of the existing collaborative threat detection techniques, such as Multi-MLP, IDSFedNet [7], and MiTFed [8] models with the proposed model. Based on this comparison, the proposed model outperforms and achieves an accuracy of 98.59% with low low-complexity model structure. The proposed model has trainable parameters of $4,042$, a model size of 15.79 KB, and an MFLOPs calculation of 0.0074. Fig. 1 presents the transaction time of the off-chain aggregation mechanism. Based on the results, the off-chain aggregation performed 9.263 ms for the average store global model time, 2.347 ms for the average access global model time, 8.995 ms for the average store local model time, and 2.217 ms for the average access local model time. The transaction time of on-chain aggregation with various consensus algorithms (QBFT, IBFT 2.0, and Ethash) is presented in Fig. 2.

IV. CONCLUSION

This paper integrates blockchain and HFL techniques to develop collaborative cyber threat detection with a verifiable off-on-chain aggregation mechanism for securing IIoT networks. Based on the measurement results, the proposed lightweight collaborative threat detection model outperforms existing techniques by achieving a high accuracy detection and has a low complexity model structure. For future work, consider delay-aware integrated private and public blockchains with a more secure model exchange 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] Z. Yu, H. Gao, X. Cong, N. Wu, and H. H. Song, "A Survey on Cyber-Physical Systems Security," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21 670–21 686, 2023.

[2] A. Zainudin, L. A. C. Ahakonye, R. Akter, D.-S. Kim, and J.-M. Lee, "An Efficient Hybrid-DNN for DDoS Detection and Classification in Software-Defined IIoT Networks," *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8491–8504, 2022.

[3] J. Zhang, C. Luo, M. Carpenter, and G. Min, "Federated Learning for Distributed IIoT Intrusion Detection using Transfer Approaches," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 7, pp. 8159–8169, 2022.

[4] M. Alazab, S. P. RM, M. Parimala, P. K. R. Maddikunta, T. R. Gadekallu, and Q.-V. Pham, "Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3501–3509, 2021.

[5] M. Abdel-Basset, N. Moustafa, and H. Hawash, "Privacy-Preserved Cyberattack Detection in Industrial Edge of Things (IEOT): A Blockchain-Orchestrated Federated Learning Approach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 7920–7934, 2022.

[6] D. C. Nguyen, M. Ding, Q.-V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12 806–12 825, 2021.

[7] 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.

[8] Z. Abou El Houda, A. S. Hafid, and L. Khoukhi, "MiTFed: A Privacy Preserving Collaborative Network Attack Mitigation Framework Based on Federated Learning using SDN and Blockchain," *IEEE Transactions on Network Science and Engineering*, 2023.