Federated Dual-Autoencoder and Blockchain-Enabled Framework for Zero-Day Intrusion Detection in IoMT

Subroto Kumar Ghosh, Mohtasin Golam, Sium Bin Noor, Jae-Min Lee, and Dong-Seong Kim
Networked Systems Laboratory, Department of IT Convergence Engineering,
Kumoh National Institute of Technology, Gumi, South Korea.
(subroto, gmoh248, siumbinmoor, ljmpaul, and dskim)@kumoh.ac.kr

***Abstract*—This paper presents a federated dual-autoencoder framework for zero-day intrusion detection in Internet of Medical Things (IoMT) environments, enhanced with permissioned blockchain logging. Each hospital trains two local autoencoders(AEs), one on normal traffic and one on attack traffic, and shares only model weights for federated averaging, preserving data privacy. The resulting global normal and attack AEs are used jointly on zero-day traffic, where a Smart-OR decision rule combines their reconstruction errors to detect anomalies. The permissioned Blockchain records model updates and detection alerts to ensure integrity and auditability of intrusion evidence. Experiments on CIC-IoMT 2024 dataset [1] achieves 85.2% accuracy and 84.93% F1-score, demonstrating that the proposed approach effectively detects zero-day attacks while respecting data locality and providing trustworthy logging.**

***Index Terms*—Autoencoder (AE), Federated Learning, IoMT, Pure Chain, Zero-day Intrusion Detection.**

I. Introduction

The rapid deployment of IoMT devices in hospitals has created highly interconnected clinical networks that are attractive targets for zero-day attacks, which exploit previously unknown vulnerabilities and can compromise patient safety and data confidentiality before patches are available [2]. Traditional perimeter defenses and signature-based IDS struggle to recognize such novel threats and are further constrained by strict privacy regulations that limit centralized collection of medical network traffic [3].

Existing research has explored AE-based anomaly detection, federated learning, and blockchain-backed security for IoT and IoMT, but these approaches are often studied in isolation or assume centralized training on aggregated datasets [2]. Many federated IDS designs rely on a single anomaly detector, making it difficult to simultaneously model benign and malicious behaviors, and they rarely provide an immutable audit trail for model evolution and intrusion alerts across multiple hospitals [3].

To address these gaps, this work introduces a federated dual-autoencoder and blockchain-enabled framework tailored for IoMT zero-day intrusion detection, where each hospital trains separate normal and attack AEs and shares only model weights for federated aggregation. The aggregated global normal and attack AEs jointly score zero-day flows using a Smart-OR rule. Pure Chain, a permissioned blockchain records model hashes and detection metadata using PoA^2 consensus [4], [5], [6], enabling privacy-preserving, collaborative detection with trustworthy evidence sharing among hospitals.

II. Methodology

Five hospitals independently preprocess their IoMT network traffic from the CIC-IoMT 2024 dataset [1], where benign flows and a subset of known attack types form the training data, and the remaining attack classes are held out as zero-day attacks for testing. Each hospital then trains two local AEs: a normal AE on its benign subset and an attack AE on its local training-attack subset, while zero-day attack classes are never exposed during training. After local convergence, each site shares only the trained AE weights with central federated server, which applies FedAvg separately to the normal and attack AEs to obtain a global normal AE and a global attack AE; scalers are aggregated or synchronized accordingly.

For zero-day detection, incoming IoMT flows from the held-out test set are transformed using the same feature extraction and scaling pipeline as in training and then reconstructed by both global AEs to compute normal and attack reconstruction errors. A Smart-OR rule flags a flow as an intrusion if the normal AE's error exceeds a tuned normal threshold or, otherwise, if the attack AE's error exceeds an attack threshold, and labels it as benign only when both conditions fail. Throughout training and detection, Pure Chain records hashes of local and global models as well as alert metadata, preventing tampering with model updates and detection logs.

III. Performance Evaluation

The proposed framework is evaluated on the CIC-IoMT 2024 dataset [1] with held-out zero-day attack scenarios to assess open-set detection capability. Using the dual global AEs with Smart-OR thresholds tuned on validation data, the framework achieves 85.2% accuracy, 85.22% precision, 84.64% recall, and 84.93% F1-score on the zero-day test split, indicating balanced detection and false-alarm performance.

The Pure Chain deployment sustains a throughput of 58.36 transactions per second with an end-to-end latency of 0.95 s, imposing lightweight overhead on on-chain operations.

The federated setting preserves data locality across hospitals without noticeable degradation compared to centralized training, while blockchain logging introduces negligible overhead relative to the end-to-end detection latency.

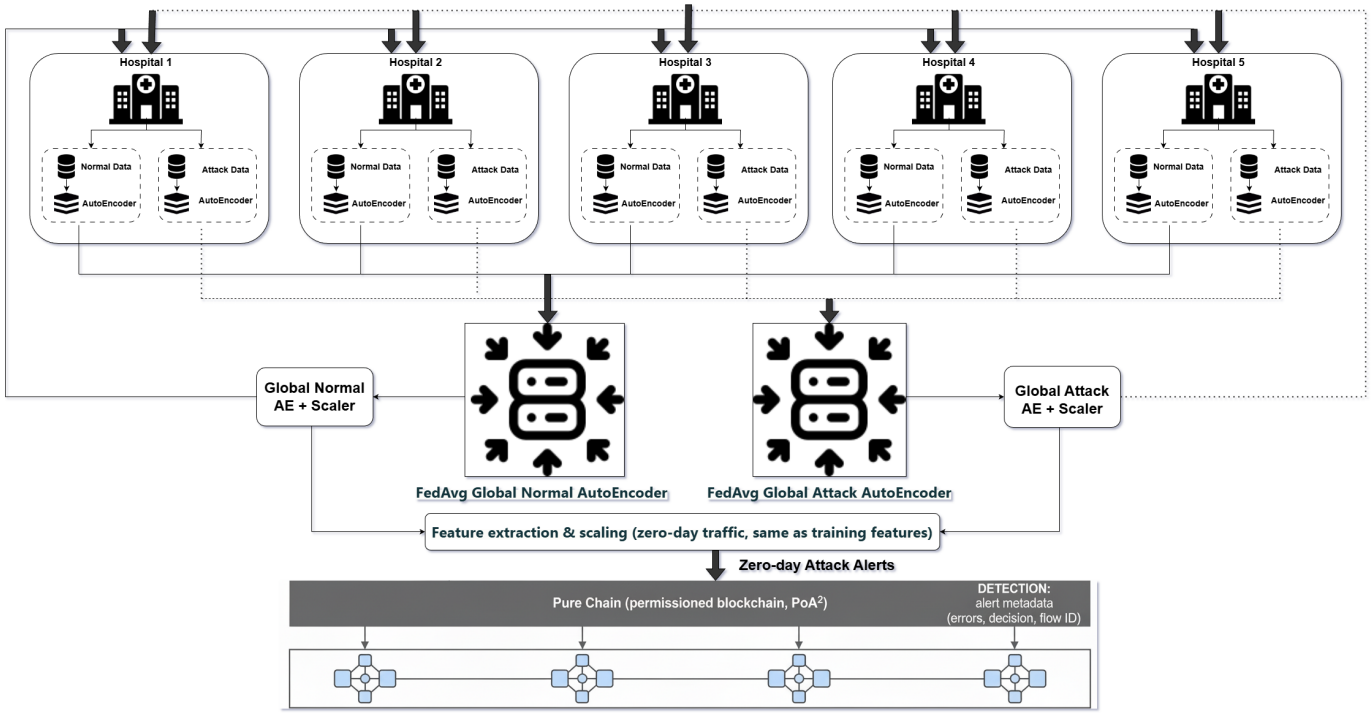

Fig. 1: Proposed Federated Dual-Autoencoder and Blockchain-Enabled Zero-Day Intrusion Detection Framework

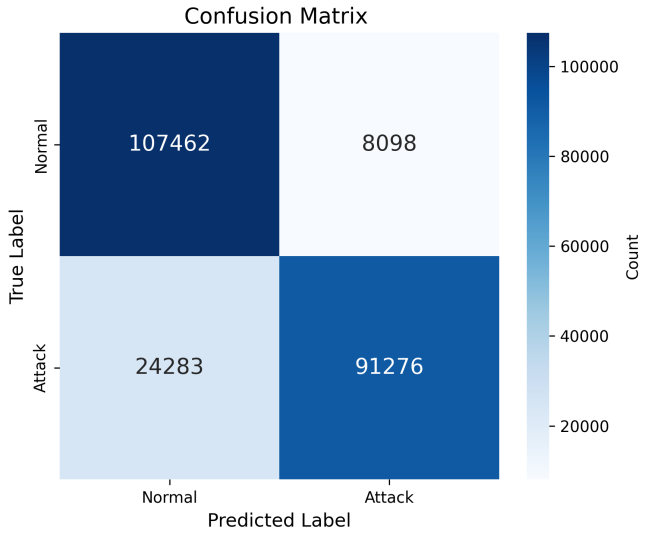

Fig. 2: Confusion matrix for the Smart-OR based zero-day detection results.

IV. Conclusion

This study demonstrates that a federated dual-autoencoder architecture, coupled with a Smart-OR decision rule, can effectively detect zero-day intrusions in IoMT networks under strict data-privacy constraints. The integration of a permissioned blockchain adds verifiable and immutable records of model evolution and intrusion alerts, strengthening trust among collaborating hospitals. Future work will extend this framework with more advanced representation learning and optimization techniques to further improve detection performance.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 33%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 34%).

References

[1] S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi, and A. A. Ghorbani, "Ciciomt2024: A benchmark dataset for multi-protocol security assessment in iomt," *Internet of Things*, vol. 28, p. 101351, 2024.

[2] U. Zukaib, X. Cui, C. Zheng, D. Liang, and S. U. Din, "Meta-fed ids: Meta-learning and federated learning based fog-cloud approach to detect known and zero-day cyber attacks in iomt networks," *Journal of Parallel and Distributed Computing*, vol. 192, p. 104934, 2024.

[3] P. Verma, N. Bharot, J. G. Breslin, D. O'Shea, A. Vidyarthi, and D. Gupta, "Zero-day guardian: A dual model enabled federated learning framework for handling zero-day attacks in 5g enabled iiot," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3856–3866, 2024.

[4] D.-S. Kim and R. Syamsul, "Integrating Machine Learning with Proof-of-Authority-and-Association for Dynamic Signer Selection in Blockchain Networks," *ICT Express*, 2024.

[5] D.-S. Kim, I. S. Igboanusi, L. A. C. Ahakonye, and G. O. Anyanwu, "Proof-of-Authority-and-Association Consensus Algorithm for IoT Blockchain Networks," in *The 43rd IEEE International Conference on Consumer Electronics (ICCE 2025)*, 2025.

[6] S. K. Ghosh, M. Golam, A. M. Tayeb, S. Bin Noor, M. S. Khaliq, J.-M. Lee, and D.-S. Kim, "Pure chain-integrated ai framework for health risk monitoring of military personnel," in *2025 International Conference on Mobile, Military, Maritime IT Convergence (ICMIC)*, 2025, pp. 258–261.