Secure Federated Learning for IoMT Intrusion Detection with Blockchain Logging

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 secure and auditable federated learning framework for intrusion detection in Internet of Medical Things (IoMT) environments. The WUSTL-EHMS-2020 healthcare monitoring dataset [1] is preprocessed using scaling and SMOTE oversampling, then trained an enhanced neural network through federated averaging across three client partitions. After each global update, model weights are serialized and hashed, and a proof of update is immutably logged on a permissioned blockchain, Pure Chain using a PoA^2 (Proof of Authority and Association) consensus mechanism for efficient, real-time recording [2], [3], [4]. The implementation achieves 96.57% accuracy and 85.49% F1-score on the test set, while Pure Chain demonstrated a transaction throughput of 18.7 transactions per second, with transaction latencies ranging from 0.7 to 1.4 seconds. By combining federated learning with blockchain logging, the proposed system enhances data privacy, model integrity, and traceability, offering a robust solution for secure, collaborative intrusion detection in IoMT networks.**

***Index Terms*—Federated learning, blockchain logging, IoMT, intrusion detection, Pure Chain, PoA^2 consensus, SMOTE.**

I. Introduction

The rapid adoption of IoMT devices enhances patient monitoring but also exposes healthcare systems to sophisticated cyberattacks. Centralized intrusion detection aggregates sensitive network data in one place, risking privacy breaches and single points of failure. Meanwhile, regulatory constraints (e.g., HIPAA, GDPR) often forbid sharing raw logs across institutions, limiting collaborative defenses [5].

Federated learning (FL) allows institutions to train a shared intrusion-detection model locally and exchange only weight updates, preserving data sovereignty. However, FL lacks mechanisms to verify update integrity or detect tampering. Current remedies centralized logs or third party auditors reintroduce trust dependencies and potential vulnerabilities [6].

This work addresses these challenges by integrating FL with Pure Chain, a permissioned blockchain platform leveraging PoA^2 consensus among authorized validators and stakeholder associations. After each FL aggregation, participants compute a cryptographic hash of the global model's serialized weights and publish it as an on-chain event. Pure Chain's rapid, secure finality produces an immutable, verifiable audit trail of model evolution. This design preserves patient privacy, prevents unauthorized tampering, and eliminates reliance on any single trusted authority in collaborative intrusion detection.

II. Methodology

The proposed framework integrates federated learning with Pure Chain-based model provenance to enable privacy-preserving intrusion detection across distributed healthcare sites, as illustrated in Figure 1.

A. Dataset and Preprocessing

The WUSTL-EHMS-2020 dataset [1] containing IoMT network traffic from hospital environments was employed. Local data at each participating site were preprocessed by normalization and noise filtering. To address class imbalance in attack categories, synthetic samples for underrepresented classes were generated using SMOTE (Synthetic Minority Over-Sampling Technique).

B. Enhanced 1D CNN Architecture

The intrusion detection model employs a 1D convolutional neural network enhanced with skip connections, batch normalization, and dropout layers. The model processes sequential IoMT traffic patterns to classify normal operations versus various attack types including denial-of-service, unauthorized access, and data exfiltration attempts.

C. Federated Learning Implementation

Each healthcare site trains the enhanced 1D CNN locally on its preprocessed data for 8 epochs. Instead of sharing raw patient data, sites transmit only model weight updates to a central federated aggregator. The aggregator applies federated averaging (FedAvg) to compute a global model, which is then redistributed to all participating sites. This iterative process continues until convergence while preserving data privacy.

D. Pure Chain-based Model Provenance

After each aggregation round, the global model weights are serialized into a byte stream and processed through SHA-256 hashing to generate a unique cryptographic fingerprint. This hash is submitted as a transaction to the Pure Chain network, secured by PoA^2 consensus. The resulting on-chain record creates an immutable, timestamped audit trail of each model update, ensuring transparency and tamper-evidence throughout the federated training process.

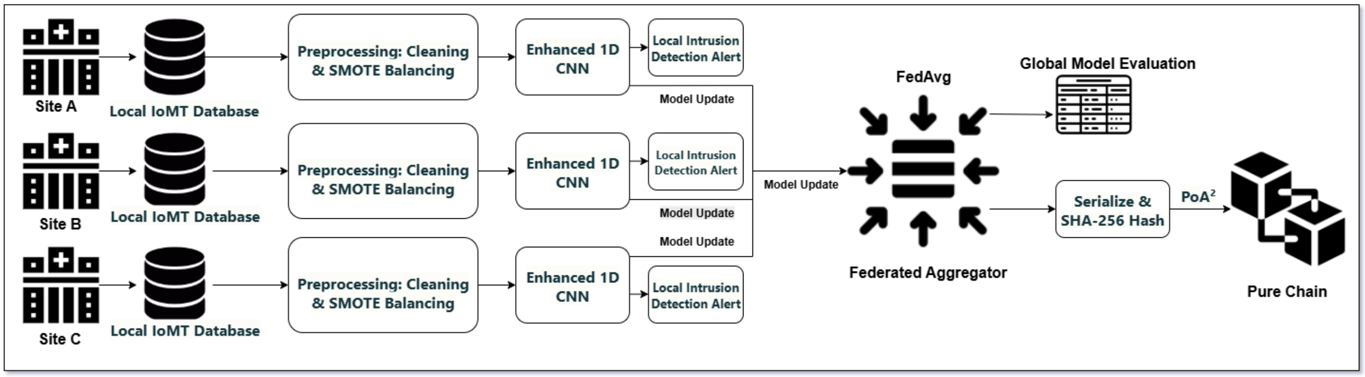

Fig. 1: System architecture of the proposed federated IoMT intrusion detection with Pure Chain-based model provenance.

TABLE I: Final Ensemble Model's Performance

Metric	Accuracy%	Precision%	Recall%	F1-score%
Value	96.57	90.91	80.68	85.49

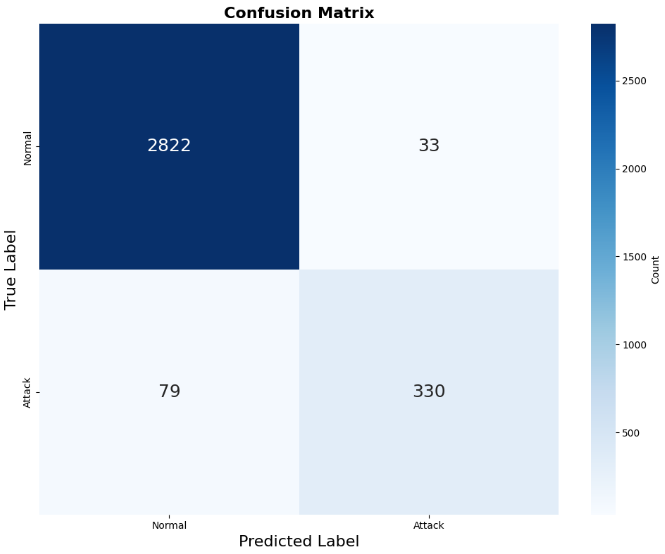

Fig. 2: Confusion matrix of the ensemble model.

III. Performance Evaluation

The proposed federated IoMT intrusion-detection framework was evaluated on a held-out test set of 3,264 samples (409 attacks). Table I reports the final ensemble's classification metrics at the optimal decision threshold (0.580). Figure 2 visualizes the confusion matrix of the ensemble's predictions.

Additionally, Pure Chain demonstrated a transaction throughput of 18.7 transactions per second with an observed latency ranging between 0.7 and 1.4 seconds, validating its capability to support real-time intrusion detection in IoMT environments.

These results demonstrate that the framework not only maintains high detection accuracy, but also ensures that patient data remains fully confidential by never sharing raw logs.

IV. Conclusion

This paper introduced a privacy-preserving, tamper-proof federated IoMT intrusion-detection framework combining FL with Pure Chain. The ensemble model achieved 96.57% accuracy and an 85.49% F1-score without sharing raw patient data, while Pure Chain delivered a throughput of 18.7 tps and latencies between 0.7 and 1.4 seconds. By recording cryptographic hashes of global updates on-chain, this work eliminates single points of trust and ensure immutable model provenance. Future work will address scalability to larger networks and explore dynamic validator selection for optimized consensus 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] Z. Rahman and S. Islam, “Effective intrusion detection in wsns: Evaluating machine learning models on wsn ds and wustl ehms-2020 datasets,” in *2025 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, 2025, pp. 1–7.

[2] 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.

[3] 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.

[4] S. K. Ghosh, M. Golam, M. S. Khaliq, M. M. H. Somrat, L. A. C. Ahakonye, J.-M. Lee, and D.-S. Kim, “Purechain for healthcare data sovereignty: Managing patient consent with smart contracts,” , pp. 1462–1463, 2025.

[5] A. Rai, M. Naik, and I. Seraphim B, “Leveraging blockchain technology for secure and efficient storage of medical data,” in *2024 IEEE 16th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2024, pp. 652–656.

[6] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, “Privacy-preserving blockchain-based federated learning for iot devices,” *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1817–1829, 2021.