PureGuard: PureChain-Orchestrated Transformer Intelligence for IIoT Security

[1]Mahbuba Iasmin Sumona, [2]Md Mehedi Hasan Somrat,[3]Dong-Seong kim,[4]Jae-Min Lee
[1,2,3,4] *Networked Systems Lab, IT convergence Engineering Department, Kumoh National Institute of Technology, Gumi, South Korea 3917.*
[4] *ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi, South Korea, 3917*
[3,4] *Networked Systems Laboratory (NSLab. Inc.), Kumoh National Institute of Technology, South Korea, 3917*
(sumona, mehedi, dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—Industrial Internet of Things (IIoT) environments demand both real-time intrusion detection and reliable security logging. This paper presents *PureGuard*, a lightweight detect-seal-log framework that integrates a compact Transformer-based intrusion detection system with *PureChain*, a gas-efficient blockchain ledger for immutable event recording. By cryptographically sealing traffic windows and selectively logging only high-confidence attacks, PureGuard achieves 98.15% detection accuracy with 0.0388 ms inference latency on the CIC-IoT-2023 dataset, while maintaining low overhead after blockchain integration.**

***Index Terms*—IIoT security, Intrusion detection, Transformer, Blockchain logging, PureChain.**

I. Introduction

The Industrial Internet of Things (IIoT) enables smart manufacturing, intelligent power grids, and automated industrial control, but increased connectivity also expands the attack surface. Attacks such as distributed denial-of-service (DDoS), protocol manipulation, and botnet infiltration pose serious operational and safety risks [1]. While deep learning–based intrusion detection systems (IDSs) achieve strong detection performance, most rely on centralized logs vulnerable to tampering after compromise [2]. Moreover, recurrent architectures such as LSTMs often fail to meet strict real-time latency constraints in industrial edge environments [3].

To ensure logging integrity, recent studies integrate IDSs with blockchain for tamper-resistant auditing [4]. However, general-purpose blockchains such as Ethereum and Hyperledger Fabric incur high transaction overhead and latency, limiting their suitability for IIoT edge deployment. Motivated by these challenges, this work proposes *PureGuard*, which jointly optimizes lightweight intrusion detection and efficient immutable logging [5]. Unlike prior IDS–blockchain approaches that rely on general-purpose ledgers or heavyweight models, PureGuard combines edge-scale Transformer inference with selective, low-gas blockchain logging in a unified detect–seal–log pipeline.

The main contributions of this paper are:

- A compact Transformer-based IDS enabling accurate multi-class IIoT attack detection with ultra-low edge inference latency.
- A detect-seal-log pipeline that cryptographically binds detected events to verifiable and tamper-resistant records.

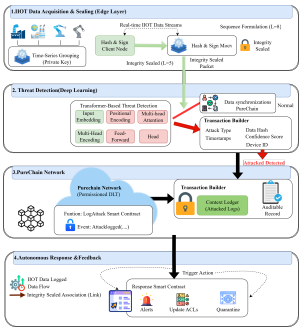

Fig. 1. PureGuard detect-seal-log pipeline deployed at the IIoT edge.

- A lightweight PureChain integration [6] providing low-cost and reliable immutable logging for real-time IIoT systems.

II. System Design and Methodology

A. System Overview

PureGuard implements a layered detect–seal–log pipeline at industrial edge gateways, as shown in Fig. 1. Incoming IIoT traffic is segmented into short windows, cryptographically sealed, classified using a lightweight Transformer-based IDS, and selectively recorded on PureChain for high-confidence attack events.

B. Integrity Sealing

Given a traffic stream S, fixed-length windows are generated as

$$X = \text{Segment}(S, L),\ L = 8, \tag{1}$$

and sealed using a cryptographic hash and digital signature:

$$H = \text{SHA256}(X),\ \sigma = \text{Sign}(H, K_{\text{priv}}). \tag{2}$$

C. Lightweight Transformer-Based Detection

PureGuard employs a compact Transformer encoder for 34-class intrusion detection using 21 selected traffic features. Multi-head self-attention captures diverse traffic patterns as

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^\top}{\sqrt{d_k}}\right)V. \tag{3}$$

III. Experimental Results

A. Dataset and Experimental Setup

PureGuard is evaluated on the CIC-IoT-2023 dataset, comprising over 46 million IoT traffic records across 34 classes [7].

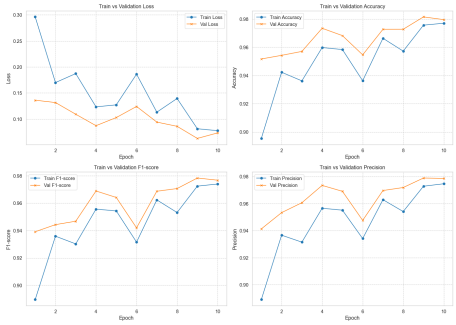

Fig. 2. Training and validation performance convergence over epochs.

TABLE I
DETECTION PERFORMANCE BEFORE AND AFTER PURECHAIN INTEGRATION

Metric	Before PureChain	After PureChain	PureChain metric
Accuracy	98.15%	97.96%	–
Precision	97.89%	97.75%	–
Recall	98.15%	97.96%	–
F1-score	97.83%	97.62%	–
ROC-AUC	99.99%	–	–
Latency (ms/sample)	0.0388	0.0411	–
Throughput (samples/sec)	22448.38	550.00	–
Logged attacks	–	–	4270
Logging success	–	–	100.00%
Avg. gas/transaction	–	–	34,274
Model size (MB)	1.84	–	–
Memory used (MB)	5.28	–	–

For efficient edge deployment, 21 discriminative features are selected, and the model converges within 10 epochs.

B. Detection Performance

The Transformer-based IDS achieves an accuracy of 98.15% prior to blockchain integration and 97.96% after PureChain logging, indicating minimal performance degradation. Fig. 2 illustrates stable training and validation convergence, while the confusion matrix in Fig. 3 confirms high precision and recall with a strong true-negative rate, thereby reducing false alarms in industrial environments.

C. Latency, Throughput, and Logging Analysis

Before blockchain integration, PureGuard achieves an inference latency of 0.0388 ms per sample. After PureChain integration, latency slightly increases to 0.0411 ms due to transaction submission, while throughput decreases because of synchronous on-chain confirmation; this overhead affects only detected attacks, as normal traffic is not logged. PureChain logs 4,270 attack events with 100% success using an average of 34,274 gas units per transaction. Compared with Ethereum or Hyperledger Fabric, PureChain avoids global consensus and smart-contract execution overhead, making it better suited for real-time IIoT edge logging.

D. Comparative Analysis

Table II compares PureGuard with CNN-based and GAN+Transformer IDSs.

TABLE II
COMPARATIVE PERFORMANCE ANALYSIS.

Model	Acc.(%)	Lat.(ms)	Tamper	Edge Suitability
Hybrid CNN–LSTM [1]	95.23	–	No	Weak
CNN [3]	95.27	1.43	No	Good
GAN+Transformer [2]	98.78	820	Yes	Good
PureGuard (Ours)	98.15	0.0388	Yes	Strong

PureGuard offers higher accuracy than CNN models and comparable accuracy to GAN+Transformer while achieving orders-of-magnitude lower latency (0.0388 ms), making it better suited for real-time IIoT edge deployment.

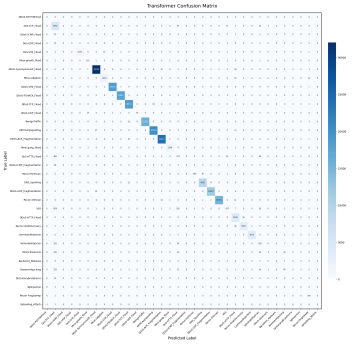

Fig. 3. Transformer confusion matrix on CIC-IoT-2023.

IV. Conclusion

This paper presented PureGuard, a lightweight IIoT intrusion detection framework that integrates a compact Transformer-based IDS with PureChain for efficient and immutable security logging. Experimental results on the CIC-IoT-2023 dataset demonstrate that high detection accuracy and ultra-low latency can be achieved while providing reliable and low-overhead forensic accountability for industrial edge environments.

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, 25%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 25%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 25%) and by Basic Science Research Program through the NRF funded by the Ministry of Education (RS-2025-25431637, 25%).

References

[1] S. K. Erskine, "Real-time large-scale intrusion detection and prevention system (idps) ciciot dataset traffic assessment based on deep learning," *Applied System Innovation*, vol. 8, no. 2, p. 52, 2025.

[2] C. Nandagopal, R. R. Kanna, K. Sangeetha, and P. Naveenkumar, "Cyber threat detection in 6g internet of things using deep learning and privacy preservation via blockchain," *International Journal of Communication Systems*, vol. 39, no. 2, p. e70356, 2026.

[3] N. Albanbay, Y. Tursynbek, K. Graffi, R. Uskenbayeva, Z. Kalpeyeva, Z. Abilkaiyr, and Y. Ayapov, "Federated learning-based intrusion detection in iot networks: Performance evaluation and data scaling study," *Journal of Sensor and Actuator Networks*, vol. 14, no. 4, p. 78, 2025.

[4] D.-S. Kim, E. A. Tuli, I. I. Saviour, M. M. H. Somrat, and X.-Q. Pham, "Blockchain-as-a-service: A pure chain approach," *Blockchain: Research and Applications*, p. 100397, 2025.

[5] 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.

[6] D.-S. Kim and S. Rizal, "Proof of authorization and association with machine learning," in *2025 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2025, pp. 1–6.

[7] W. A. H. Salman and C. H. Yong, "Overview of the ciciot2023 dataset for internet of things intrusion detection systems," *Mesopotamian Journal of Big Data*, vol. 2025, pp. 50–60, 2025.