Deep Learning-based PureChain-backed Robust Intrusion Detection System for Industrial IoT

[1]Mahbuba Iasmin Sumona, [2]Esmot Ara Tuli,[3]Md Mehedi Hasan Somrat,[4]Dong-Seong kim,[5]Jae-Min Lee
[1,3,4,5] *Networked Systems Lab, IT convergence Engineering Department, Kumoh National Institute of Technology, Gumi, South Korea 3917.*
[2,4] *ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi, South Korea, 3917*
[4,5] *Networked Systems Laboratory (NSLab. Inc.), Kumoh National Institute of Technology, South Korea, 3917*
(sumona, esmot, mehedi, dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—The proliferation of the Industrial Internet of Things (IIoT) across critical infrastructure demands real-time intrusion detection systems (IDS) that guarantee both high accuracy and data integrity against sophisticated cyber threats. This paper introduces the Deep Learning Integrated PureChain Model (DLI-PCM), a novel, low-latency framework for robust anomaly detection and verifiable logging in IIoT edge environments. The system's core is an LSTM-based IDS that effectively captures complex temporal dependencies in high-dimensional time-series data, achieving superior detection performance with an Accuracy of 0.9960 and an F1-Score of 0.9596. Crucially, when an attack is detected by the LSTM core, the DLI-PCM immediately generates a real-time alert, which is then secured by a specialized PureChain Data Sharing Layer utilizing a gas-free PoA^2 consensus mechanism. This unique layer ensures all detection alerts and corresponding data hashes are immediately and immutably logged via a Smart Contract, providing a tamper-proof, auditable record. Performance metrics validate its operational efficiency, showing an low Average Latency of 0.114s for transaction logging and highly cost effective due to its low transaction gas cost, thus establishing a comprehensive, trustworthy defense-in-depth strategy essential for secure Industry 4.0 environments.**

***Index Terms*—Deep Learning (DL), Industrial IoT (IIoT), Intrusion Detection System (IDS), LSTM, PureChain**

I. Introduction

The convergence of Operational Technology (OT) and Information Technology (IT) in Industrial Internet of Things (IIoT) ecosystems has enabled unprecedented levels of automation, real-time monitoring, and data-driven decision-making across critical infrastructure. This integration, however, has simultaneously expanded the cyberattack surface, exposing interconnected industrial components to adversarial manipulation capable of disrupting operational continuity, damaging equipment, or compromising safety [1]. As IIoT deployments continue to scale in heterogeneity and connectivity, the need for intrusion detection mechanisms that can operate reliably under stringent industrial constraints becomes increasingly urgent [2].

Traditional intrusion detection systems (IDS) particularly signature-based and rule-driven approaches are ill-suited for modern IIoT environments. They struggle against dynamic, stealthy, and high-dimensional attack patterns that evolve rapidly and often evade static detection logic. In contrast, deep learning (DL) techniques have demonstrated strong potential in modeling temporal and contextual dependencies within IIoT telemetry, enabling the identification of previously unseen or subtle anomalies [3] [2].

Yet, despite these advantages, contemporary DL-based IDS solutions exhibit two critical limitations. First, most rely on centralized detection or logging infrastructures, creating single points of failure that sophisticated attackers can exploit to modify, erase, or forge forensic records [4]. Second, many proposals are validated only in offline or simulated settings, without accounting for the real-world constraints of industrial systems where processing power, communication bandwidth, and latency budgets are highly restricted [5].

Existing IDS designs attempt to increase detection accuracy by employing complex deep architectures such as layered LSN, CLA, SSAE, and HGS pipelines that achieve strong modeling capacity but introduce computational overhead incompatible with resource-limited edge devices [6]. Conversely, lightweight statistical methods reduce latency but suffer from elevated false-negative rates, leaving critical operational windows unprotected. In parallel, reliance on centralized Security Information and Event Management (SIEM) infrastructures amplifies forensic vulnerability by enabling attackers to tamper with or remove log records forensics [7].

To address these challenges, this paper introduces the Deep Learning Integrated PureChain Model (DLI-PCM), a unified framework that couples low-latency LSTM-based anomaly detection with a decentralized, tamper-resistant blockchain logging layer. The LSTM component captures fine-grained temporal dynamics in IIoT traffic to enable accurate real-time threat classification, while the PureChain layer employs a low gas PoA² consensus mechanism to ensure immutable, verifiable, and cost-efficient recording of intrusion alerts [8] [7]. This integration eliminates the single-point-of-failure limitation of centralized logging and enhances forensic traceability during and after security incidents.

The key contributions of this work are as follows:

1) Introduction of the DLI-PCM architecture, which integrates LSTM-based threat detection with a decentralized blockchain layer for data integrity
2) Real-time threat classification, achieved through the deployment of LSTM networks on edge devices, enabling low-latency, high-accuracy detection of anomalies.

3) Immutable data logging, facilitated by the PureChain blockchain, which guarantees the integrity and non-repudiation of detection alerts through a almost gas-free PoA2 consensus mechanism.
4) Empirical validation, demonstrating the superior performance of the DLI-PCM system compared to existing IDS approaches in terms of detection accuracy, latency, and cost-effectiveness.

II. Related Work

The increasing interconnection of OT and IT systems within IIoT infrastructures has prompted extensive research into cybersecurity mechanisms tailored for industrial environments. Two predominant research directions Deep Learning–based intrusion detection and blockchain-enabled integrity preservation have demonstrated substantial potential but also revealed significant shortcomings when considered independently.

A. Deep Learning-Based IDS in IIoT

Deep learning techniques have been widely adopted for anomaly detection across IIoT systems due to their capability to automatically learn hierarchical representations from diverse telemetry sources. Hybrid models that combine CNNs for spatial pattern extraction, LSTMs or GRUs for temporal sequence modeling, and autoencoders for unsupervised anomaly detection have achieved state-of-the-art accuracy in benchmark datasets [1].Furthermore, attention mechanisms and ensemble learning have been explored to enhance robustness against stealthy attacks.

However, these methods typically require substantial computational resources, limiting their suitability for deployment in edge nodes with restricted CPU, memory, and energy budgets. High inference latency also undermines their effectiveness in environments requiring sub-second response times [1]. Additionally, the lack of explainability in many deep learning architectures presents challenges in mission-critical IIoT applications, where operators must interpret and justify anomaly classifications. Only a limited subset of research evaluates these systems under real-world industrial constraints, such as fluctuating traffic loads, noisy sensor data, or hardware limitations.

B. Blockchain for IIoT Security and Trust

Blockchain has emerged as a decentralized mechanism capable of ensuring data immutability, secure event logging, and transparent forensic trails in IIoT networks. Prior efforts have utilized Ethereum smart contracts, Hyperledger Fabric's permissioned consensus, and customized private blockchains to store network events, authenticate device interactions, and verify access control [9].While these approaches demonstrate improved trust management, their operational overhead raises concerns.

Public blockchains suffer from high latency and transaction fees, making them impractical for real-time or high-frequency logging. Permissioned blockchains, though more efficient, still incur communication overhead and may not fully support synchronous integration with detection systems. Notably, most existing blockchain-enabled IDS solutions log events only after detection, resulting in delays that expose the system to tampering risks. The PureChain framework addresses some of these limitations by offering gas-free transactions and a PoA² consensus mechanism designed to reduce computational burden and latency [10] [7].

C. Research Gaps

Although deep learning improves detection and blockchain strengthens forensic integrity, current research still lacks a unified framework for the complex security needs of IIoT systems.. Prior work has not simultaneously integrated:

1) Low-latency deep learning-based detection at the edge,
2) Immediate and verifiable blockchain-backed alert logging, and
3) Systematic evaluation framework that approximates real-world industrial operational constraints through empirical latency analysis, resource-aware model design, and attack-driven workload simulation.

In practice, fully reproducing industrial operating conditions such as heterogeneous device capabilities, dynamic network congestion, and safety-critical response deadlines is challenging in a controlled research environment. Accordingly, rather than full-scale deployment, this work analytically models key constraints and evaluates the system via realistic latency measurements, throughput profiling, and resource-bounded deep learning inference that approximate industrial execution characteristics [4].

The proposed Deep Learning Integrated PureChain Model (DLI-PCM) aims to fill this gap by integrating an LSTM-based edge detector with a lightweight blockchain layer, enabling real-time intrusion detection alongside tamper-proof forensic auditing.

III. Methodology

Consequently, there remains a clear need for an IIoT intrusion detection architecture that couples high detection performance with verifiable log integrity, while ensuring computational feasibility and responsiveness under experimentally derived constraint conditions. The proposed Deep Learning Integrated PureChain Model (DLI-PCM) addresses this gap by integrating an LSTM-based anomaly detector with a lightweight PoA²-enabled blockchain layer. This architecture enables real-time threat identification and tamper-proof alert recording, while its empirical evaluation provides a reproducible methodology for understanding how such a system would behave under quasi-realistic industrial workloads.

A. Proposed System Architecture

Figure 1 illustrates the end-to-end operational flow of the proposed security framework. Heterogeneous IIoT devices and edge-layer sensors continuously emit high-dimensional telemetry streams comprising network statistics, protocol-level metadata, temporal flow descriptors, and packet-oriented attributes. These raw measurements are first routed to the

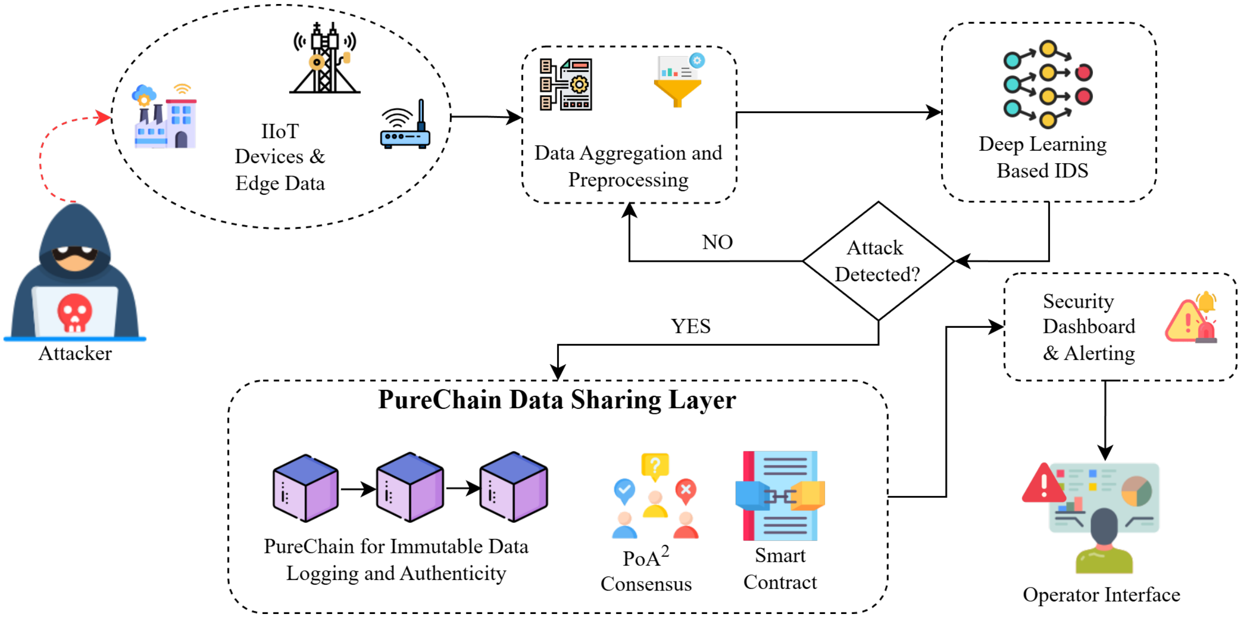


Fig. 1. Proposed System Diagram of Deep Learning Integrated PureChain IDS Model.

Data Aggregation and Preprocessing Module, which performs cleansing, normalization, and feature structuring to transform unrefined traffic into analytically coherent vectors suitable for subsequent deep learning inference [11].

The resulting feature representations $\mathbf{x}_t$ are then processed by the Deep Learning–based Intrusion Detection System (IDS), which evaluates sliding windows of IIoT activity to determine whether the observed state corresponds to legitimate operational behavior or a deviation indicative of an attack. Upon classification, the system branches according to the IDS decision output: if $\hat{y}_t$ = benign, the data stream continues through the standard processing pipeline without interruption; if $\hat{y}_t$ = attack, the detection event triggers two simultaneous actions.

First, the alert is communicated to the Security Dashboard and Operator Interface, enabling real-time situational awareness and facilitating rapid response. Second, the event and its associated metadata are transmitted to the PureChain Data-Sharing Layer. This layer employs an immutable logging mechanism supported by a PoA^2 consensus scheme and smart-contract-driven validation to ensure trustworthy, tamper-resistant record-keeping. Through this dual response pathway, the architecture provides both operational continuity and verifiable forensic traceability whenever anomalous activity is detected [8] [7].

B. Deep Learning Core for Anomaly Detection

Let the IIoT state at time t be a multivariate feature vector $\mathbf{X}_t \in \mathbb{R}^d$, where d denotes the number of features. Using a fixed window size k, the IDS constructs temporal sequences

$$\mathbf{W}_t = [\mathbf{X}_{t-k+1}, \ldots, \mathbf{X}_t]. \tag{1}$$

These sequences are fed into a Long Short-Term Memory (LSTM) network designed to capture long-range temporal dependencies typical of evolving IIoT traffic patterns. The LSTM unit computes its internal states using

$$\mathbf{f}_t = \sigma\big(W_f[\mathbf{h}_{t-1}, \mathbf{X}_t] + \mathbf{b}_f\big), \tag{2}$$

$$\mathbf{i}_t = \sigma\big(W_i[\mathbf{h}_{t-1}, \mathbf{X}_t] + \mathbf{b}_i\big), \tag{3}$$

$$\tilde{\mathbf{c}}_t = \tanh\big(W_c[\mathbf{h}_{t-1}, \mathbf{X}_t] + \mathbf{b}_c\big), \tag{4}$$

$$\mathbf{c}_t = \mathbf{f}_t \odot \mathbf{c}_{t-1} + \mathbf{i}_t \odot \tilde{\mathbf{c}}_t, \tag{5}$$

$$\mathbf{h}_t = \mathbf{o}_t \odot \tanh(\mathbf{c}_t), \tag{6}$$

where $\sigma(\cdot)$ is the sigmoid activation, $\odot$ denotes element-wise multiplication, and $W_{\{\cdot\}}$, $\mathbf{b}_{\{\cdot\}}$ are trainable weight matrices and bias vectors, respectively. A final dense layer outputs the attack probability. The binary decision is made via a thresholding function

$$\hat{y}_t = \begin{cases} 1, & \text{if } p(\text{attack} \mid \mathbf{W}_t) > \tau, \\ 0, & \text{otherwise}, \end{cases} \tag{7}$$

where τ is a decision threshold, is empirically selected using validation-set optimization based on ROC and F1-score analysis, ensuring an optimal balance between false positives and false negatives under IIoT operational constraints.

C. PureChain Data Sharing Layer for Immutable Logging

Upon detection of an anomaly ($\hat{y}_t = 1$), DLI-PCM generates an intrusion payload P containing metadata such as timestamps, device identifiers, suspected attack type, and the LSTM confidence score. To ensure tamper resistance, the payload is hashed using

$$H_P = \text{SHA-256}(P). \tag{8}$$

The system then constructs a signed transaction

$$T = \{P,\, H_P,\, \text{Sign}(H_P, SK_{\text{edge}})\}, \tag{9}$$

where SK_{edge} denotes the private key of the authenticated edge node. This transaction is forwarded to the PureChain Data Sharing Layer, which implements the PoA^2 (Proof-of-Authority-and-Association) consensus. The consensus nodes validate the signature and append the alert as part of a new block

$$B_i = \{H_{i-1}, T, \text{MerkleRoot}, \text{Timestamp}\}. \quad (10)$$

As represented in Figure 1, the PureChain layer provides (i) immutable data logging, (ii) authenticity verification, and (iii) automated access control and alert generation via smart contracts. This makes the final logged event resistant to retrospective modification or deletion.

D. Real-Time Alerting and Operator Interface

Following successful block formation, the smart contract triggers an *Alert Event*, which is propagated to the Security Dashboard and Operator Interface in Figure 1. The dashboard displays the hash reference, block details, and attack metadata, enabling operators to perform immediate mitigation and forensic analysis. The end-to-end system latency is expressed as

$$\lambda_{\text{total}} = \lambda_{\text{det}} + \lambda_{\text{chain}}, \quad (11)$$

where λ_{det} is the LSTM inference time and λ_{chain} denotes the PureChain logging latency.

IV. Experimental Results and Discussion

A. Dataset and Experimental Setup

The proposed DLI-PCM model is evaluated on the Edge-IIoTset dataset [11], which contains 61 features and 14 attack categories. All numerical features are standardized to zero mean and unit variance, and time-ordered flow records are grouped into sequences of length $k = 20$. The dataset is split chronologically into 70%/15%/15% for training, validation, and testing, respectively, to avoid temporal leakage. Class imbalance is addressed using a class-weighted binary cross-entropy loss. The LSTM classifier comprises two stacked layers with 128 and 64 hidden units and a dropout rate of 0.3, followed by a sigmoid output layer. Training is performed using the Adam optimizer (learning rate 10^{-3}), a batch size of 128, and early stopping based on the validation loss. All experiments are conducted in Python with TensorFlow on a GPU-enabled workstation. The PureChain layer is deployed with three PoA^2 validator nodes to measure on-chain logging latency and throughput.

B. Evaluation Metrics

We conducted validation and testing on the dataset to ensure that the proposed LSTM model was supplied with the trained parameters and executed over 20 epochs. As a result, the complete model achieved 99.60% accuracy for both training and validation, as illustrated in Figure 2. Likewise, the model exhibited a validation loss of only 0.0353% after 20 epochs, as shown in Figure 3. The trained model, which incorporates large-scale IoT device data, was subsequently finalized and optimized using the EdgeIIoT dataset. The optimization strategy accounted for computational feasibility and the maximum achievable accuracy of the proposed LSTM architecture. Furthermore, this phase signified the completion of the intrusion-detection mechanism, effectively addressing the intrusion attacks originally present in the EdgeIIoT dataset. The proposed LSTM-based Intrusion Detection System (IDS), evaluated on the EdgeIIoT dataset, demonstrates strong classification performance as summarized in the Table I

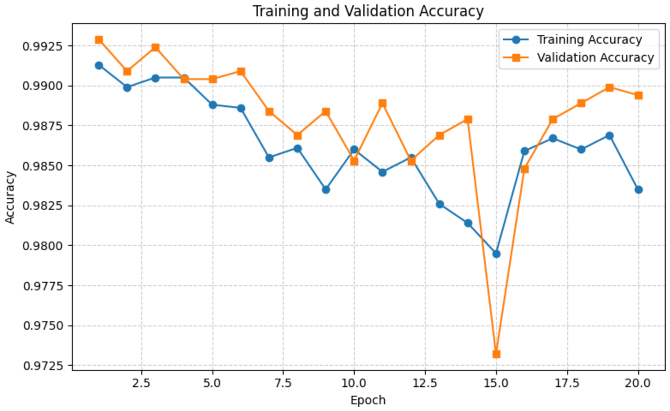


Fig. 2. Training and Validation Accuracy for each Epoch

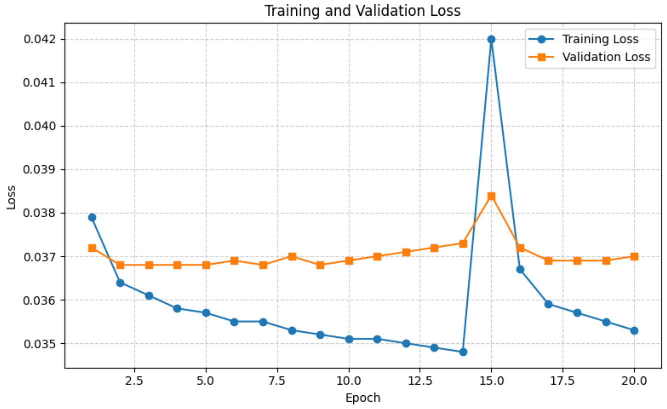


Fig. 3. Training and Validation loss for each Epoch

TABLE I
PERFORMANCE METRICS FOR LSTM MODEL ON EDGEIIOT IDS

Model	LSTM
Accuracy	0.9960
Precision	0.9725
Recall	0.9689
F1-Score	0.9596
Training Time (s)	34.975
Testing Time (s)	0.4900
Inference Time (s)	0.0591

The model achieved an accuracy of 0.9960, with precision, recall, and F1-score each at 0.9596. These values reflect the system's high proficiency in distinguishing anomalous from benign activity, with minimal error rates. Additionally, the training time of approximately 34.98 seconds and very low testing and inference times 0.49 seconds and 0.059 seconds, respectively, indicate that the system offers both effectiveness and efficiency suitable for real-time IIoT threat detection scenarios [12].

Classification Metrics

Accuracy (Acc) measures the overall correctness of model predictions, calculated as the ratio of correctly classified samples (both normal and attack) to the total number of samples:

$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \tag{12}$$

Precision (P) indicates how many predicted attacks are true, reflecting the model's ability to avoid false alarms:

$$P = \frac{TP}{TP + FP} \tag{13}$$

Recall (R) measures how many actual attacks were detected, representing the model's sensitivity to intrusions:

$$R = \frac{TP}{TP + FN} \tag{14}$$

F1-Score ($F1$) is the harmonic mean of precision and recall, balancing the trade-off between false positives and false negatives.

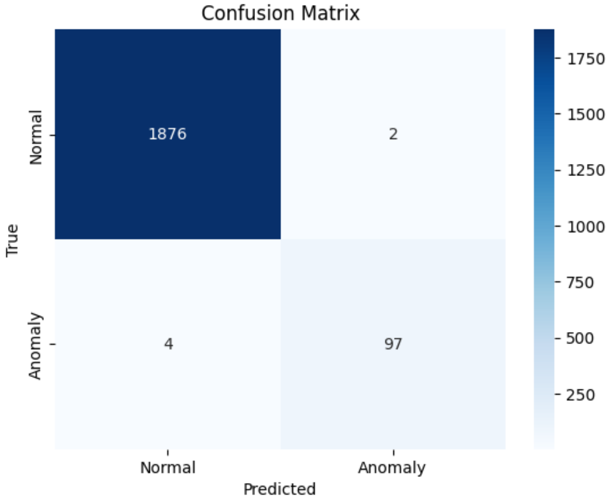


Fig. 4. Confusion matrix of the IDS model on the EdgeIIoT dataset.

The Figure 4 confusion matrix summarises the IDS model's classification outcomes for normal and anomalous events using the EdgeIIoT dataset. The diagonal cells (1876 and 97) represent correctly classified samples: normal instances in the upper left and anomalies in the lower right. Off-diagonal entries (2 false positives, 4 false negatives) indicate misclassifications. Overall, the matrix reveals high accuracy and robust anomaly detection capability, with minimal false alarms and missed detections.

C. Evaluation of PureChain's Immutable Logging

PureChain ensures tamper-proof, auditable IIoT intrusion logs by storing each detected attack as a unique blockchain transaction.

The latency reported in fig.5, corresponds to the delay between the occurrence of an event and its on-chain registration, rather than the detection time of the deep learning model. The Alert Log records unique attack identifiers (e.g., IDs 20 and 271) and their transaction hashes (TxHash), confirming successful on-chain commitment. The observed logging latencies range from 0.096 s (Attack 20) to 0.736 s (Attack 192), indicating near real-time transaction finality while revealing the quantitative impact of blockchain communication overhead and network congestion on system responsiveness.

Table II summarises the PureChain logging results during real-time IDS operation. All detected attacks were successfully registered on PureChain, with no failures. The system achieved an average transaction latency of 0.114 seconds and a throughput of 34.64 transactions per second, demonstrating suitability for high-throughput environments.

TABLE II
PURECHAIN LOGGING PERFORMANCE SUMMARY

Metric	**Value**
Total attacks detected	99
Successfully logged	99
Failed logs	0
Average latency per tx (s)	0.114
Throughput (TPS)	34.64

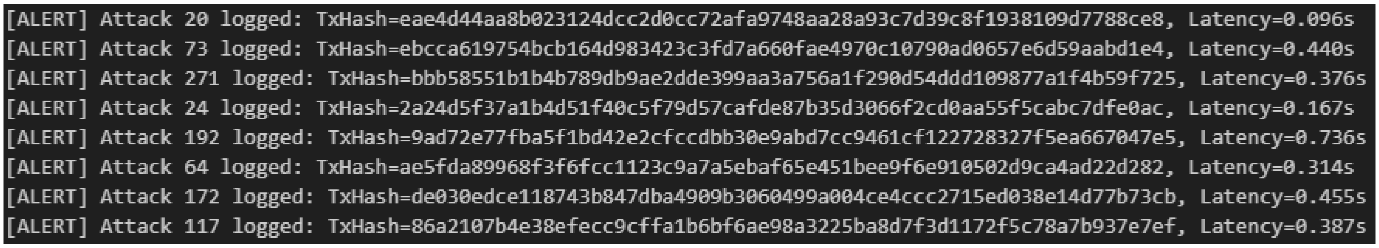
These results confirm that PureChain provides highly reliable and efficient logging, making it well-suited to real-time intrusion detection deployments in edge and IIoT environments.

D. Comparative Analysis

A consolidated comparison of all evaluated IDS models highlights the clear performance and operational advantage of the proposed LSTM-based architecture, as shown in Table III. The CNN-GRU-LSTM model [13] achieves moderate accuracy (0.960) and F1-score (0.932), but its Purechain logging latency of $0.257\,$s reflects substantial overhead from its layered convolutional–recurrent design, limiting its real-time usability. Similarly, the Ethereum-based CNN model [14] yields lower accuracy (0.989), precision (0.936), and F1-score (0.936), alongside an even higher latency of $0.257\,$s, underscoring its reduced suitability for time-sensitive IIoT tasks.

The Isolation Forest model, despite achieving the lowest latency ($0.032\,$s) with PureChain logging, demonstrates weaker accuracy (0.897) and F1-score (0.866), illustrating the challenges of unsupervised detection in noisy IIoT environments. The MARL-FL model [15] shows strong accuracy (0.990) and F1-score (0.988) but still incurs comparatively high latency and lacks tamper-resistant auditability.

In contrast, the proposed LSTM achieves the highest accuracy (0.996) and a competitive F1-score (0.959) while maintaining a substantially lower PureChain latency of $0.114\,$s.



```
[ALERT] Attack 20 logged: TxHash=eae4d44aa8b023124dcc2d0cc72afa9748aa28a93c7d39c8f1938109d7788ce8, Latency=0.096s
[ALERT] Attack 73 logged: TxHash=ebcca619754bcb164d983423c3fd7a660fae4970c10790ad0657e6d59aabd1e4, Latency=0.440s
[ALERT] Attack 271 logged: TxHash=bbb58551b1b4b789db9ae2dde399aa3a756a1f290d54ddd109877a1f4b59f725, Latency=0.376s
[ALERT] Attack 24 logged: TxHash=2a24d5f37a1b4d51f40c5f79d57cafde87b35d3066f2cd0aa55f5cabc7dfe0ac, Latency=0.167s
[ALERT] Attack 192 logged: TxHash=9ad72e77fba5f1bd42e2cfccdbb30e9abd7cc9461cf122728327f5ea667047e5, Latency=0.736s
[ALERT] Attack 64 logged: TxHash=ae5fda89968f3f6fcc1123c9a7a5ebaf65e451bee9f6e910502d9ca4ad22d282, Latency=0.314s
[ALERT] Attack 172 logged: TxHash=de030edce118743b847dba4909b3060499a004ce4ccc2715ed038e14d77b73cb, Latency=0.455s
[ALERT] Attack 117 logged: TxHash=86a2107b4e38efecc9cffa1b6bf6ae98a3225ba8d7f3d1172f5c78a7b937e7ef, Latency=0.387s
```

Fig. 5. Successful attack alerts and PureChain logging

This balance demonstrates its efficiency in modeling temporal dependencies and generating concise, verifiable blockchain-logged alerts.Overall, the comparative analysis identifies the proposed LSTM as the most effective model, offering the strongest combination of detection performance, computational efficiency, and secure blockchain-based auditability.

TABLE III
COMPARATIVE PERFORMANCE OF IDS MODELS

Model	Accuracy	F1-Score	Precision	Latency
CNN–GRU–LSTM	0.960	0.932	0.962	0.257 s
CNN	0.989	No	0.936	0.257 s
Isolation Forest	0.897	0.866	0.872	0.032 s
MARL-FL	0.990	0.988	0.989	5.200 s
Proposed LSTM	**0.996**	**0.959**	**0.972**	**0.114 s**

V. CONCLUSION

This paper introduced DLI-PCM, an LSTM-based intrusion detection framework integrated with PureChain PoA^2 blockchain logging for securing Industrial IoT environments. Using the Edge-IIoTset dataset, the model achieved an accuracy of 0.9960 with an average inference time of 0.059 s, while PureChain recorded alerts with a logging latency of 0.114 s and a throughput of 34.64 TPS. These results demonstrate that combining deep learning with a lightweight blockchain layer can provide both accurate detection and low-latency, tamper-proof alert recording. The current study is limited to binary attack classification and a single deployment setting. Future work will extend the model to multiclass attack detection, evaluate robustness across multiple datasets, and further optimize PureChain parameters to improve scalability and reduce logging overhead in diverse IIoT scenarios.

ACKNOWLEDGEMENT

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 National Research Foundation of Korea(NRF) funded by the Ministry of Education(RS-2025-25431637, 25%).

REFERENCES

[1] A. Orman, "Cyberattack detection systems in industrial internet of things (iiot) networks in big data environments," *Applied Sciences*, vol. 15, no. 6, p. 3121, 2025.

[2] M. Al Rawajbeh, A. J. Maria Soosai, L. K. Ramasamy, and F. Khan, "Trustworthy adaptive ai for real-time intrusion detection in industrial iot security," *IoT*, vol. 6, no. 3, p. 53, 2025.

[3] S. M. S. Bukhari, M. H. Zafar, M. Abou Houran, Z. Qadir, S. K. R. Moosavi, and F. Sanfilippo, "Enhancing cybersecurity in edge iiot networks: An asynchronous federated learning approach with a deep hybrid detection model," *Internet of Things*, vol. 27, p. 101252, 2024.

[4] N. Alkhafaji, T. Viana, and A. Al-Sherbaz, "Integrated genetic algorithm and deep learning approach for effective cyber-attack detection and classification in industrial internet of things (iiot) environments," *Arabian Journal for Science and Engineering*, pp. 1–25, 2024.

[5] B. Ahmad, Z. Wu, Y. Huang, and S. U. Rehman, "Enhancing the security in iot and iiot networks: An intrusion detection scheme leveraging deep transfer learning," *Knowledge-Based Systems*, vol. 305, p. 112614, 2024.

[6] A. Banitalebi Dehkordi, "Edblsd-iiot: a comprehensive hybrid architecture for enhanced data security, reduced latency, and optimized energy in industrial iot networks," *The Journal of Supercomputing*, vol. 81, no. 2, p. 359, 2025.

[7] 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.

[8] 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 *2025 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2025, pp. 1–6.

[9] M. Rodriguez, D. P. Tobon, and D. Munera, "A framework for anomaly classification in industrial internet of things systems," *Internet of Things*, vol. 29, p. 101446, 2025.

[10] M. I. Hossain, T. Steigner, M. I. Hussain, and A. Akther, "Enhancing data integrity and traceability in industry cyber physical systems (icps) through blockchain technology: A comprehensive approach," *arXiv preprint arXiv:2405.04837*, 2024.

[11] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-iiotset: A new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning," *IEEe Access*, vol. 10, pp. 40 281–40 306, 2022.

[12] A. Quraishi, M. A. Rusho, A. Prasad, I. Keshta, R. Rivera, and M. W. Bhatt, "Employing deep neural networks for real-time anomaly detection and mitigation in iot-based smart grid cybersecurity systems," in *2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*. IEEE, 2024, pp. 1–6.

[13] C. A. Nnadiekwe, S. O. Ajakwe, J. M. Lee, and D.-S. Kim, "Remote-care: Ai-driven multimodal predictive framework with blockchain for personalized remote patient monitoring in iomt," *IEEE Internet of Things Journal*, pp. 1–1, 2025.

[14] M. F. Rahaman, M. Golam, M. R. Subhan, E. A. Tuli, D.-S. Kim, and J.-M. Lee, "Meta-governance: Blockchain-driven metaverse platform for mitigating misbehavior using smart contract and ai," *IEEE Transactions on Network and Service Management*, vol. 21, no. 4, pp. 4024–4038, 2024.

[15] G. Alandjani, "A marl-federated blockchain-based quantum secure framework for trust management in industrial internet of things," *Scientific Reports*, vol. 15, no. 1, p. 39149, 2025.