SecureEdgeNet:PureChain-Integrated Deep Learning Architecture for IIoT Cyber Defense

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

***Abstract*—The rapid proliferation of Industrial Internet of Things (IIoT) has introduced significant cybersecurity risks to smart factories and industrial control environments. This work presents SecureEdgeNet, a novel cyber defense framework combining Purechain and LSTM-based intrusion detection at the edge. The proposed architecture ensures robust anomaly detection, decentralized trust, and tamper-proof data integrity with minimal resource overhead, advancing the state of cyber resilience in IIoT systems. SecureEdgeNet was validated using benchmark IIoT datasets. The LSTM model demonstrated outstanding performance, achieving an accuracy of 98.94%,Comparisons with a baseline Isolation Forest model showed superior performance in accuracy 97.59%.**

***Index Terms*—Cybersecurity, Deep Learning, Edge Computing, Industrial Internet of Things (IIoT),Intrusion Detection,LSTM, PureChain.**

I. Introduction

Industrial IoT is redefining manufacturing and critical infrastructure by connecting diverse sensors, actuators, and control platforms through ubiquitous networks. However, this paradigm increases the attack surface ranging from targeted malware to advanced persistent threats posing direct risks to operational safety and data confidentiality [1]. Traditional security solutions lack both scalability and adaptability in highly dynamic IIoT environments, necessitating advanced methods for threat detection and trust management [2]. Blockchain technologies such as Purechain offer unique advantages for securing IIoT by ensuring transparency, decentralization, and tamper resistance for critical event data and access policies [2],[3]. Deep learning approaches especially LSTM models demonstrate superior performance in capturing temporal threat patterns within network telemetry and IIoT data [4].This paper presents two key contributions:

- An edge-centric architecture combining Purechain's blockchain with high-accuracy LSTM models for real-time threat detection and traceability in IIoT environments.
- A secure framework for model provenance and event auditability, ensuring data integrity and transparency through Purechain smart contracts with minimal latency.

II. System Architecture

Figure 1 illustrates the system architecture, depicting data flow from IIoT sensors to LSTM-based intrusion detection and blockchain logging. The SecureEdgeNet architecture seamlessly integrates data from industrial sensors and SCADA systems, which undergoes preprocessing steps such as filtering, normalization, and feature extraction. The processed data is then fed into an LSTM-based deep learning module designed for effective intrusion detection[4]. Any detected anomalies are recorded and securely stored on the Purechain layer, utilizing distributed ledgers and smart contracts to guarantee data integrity and transparency[5]. This integration ensures that the system remains tamper-proof and verifiable. An admin dashboard is employed to retrieve and display the blockchain logs in real-time, providing continuous monitoring and auditing capabilities, which enhance system security and operational oversight.

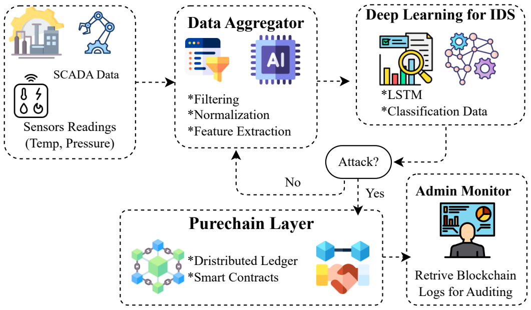


Fig. 1. SecureEdgeNet system architecture for IIoT intrusion detection system

A. Advanced Anomaly Detection System for IIoT

This study used the Edge-IIoTset dataset with 14 attack types and normal traffic [6]. It applied a deep learning model for temporal intrusion detection and an unsupervised tree-based model for rare anomalies [7], with all detection results securely logged on Purechain for immutable and auditable records.

B. Purechain for Immutable Log

The smart contract acts as a tamper-proof ledger on the Purechain blockchain, recording intrusion detection alerts and model updates as immutable events. Only authorized administrators can log data, ensuring secure and auditable tracking of security events. This contract supports changing admin rights for flexible governance, providing transparency and trust

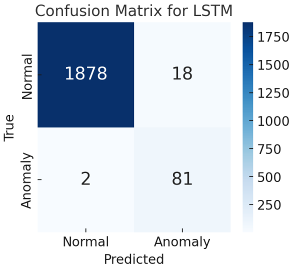


Fig. 2. Confusion Metrics for LSTM Model

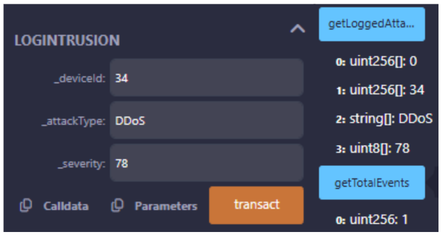
within the SecureEdgeNet system. The contract operates on a Permissioned Proof-of-Authority-and-association consensus mechanism PoA^2[3], which uses a small set of trusted validators to efficiently confirm transactions with low latency and high throughput.

III. Evaluation and Results

SecureEdgeNet was validated using EdgeIIoT[6] datasets and simulated industrial environments. The deployed LSTM model demonstrated outstanding performance. Table I compares key performance metrics between the proposed LSTM and a baseline Isolation Forest model. LSTM outperforms Isolation Forest across all metrics, particularly in recall and F1-Score. Figure 2 presents confusion matrix values for both models on the binary classification task. The LSTM achieves higher true positive and true negative detections, with fewer false negatives, highlighting its superior threat identification capability. The high accuracy underlines strong classification of benign and attack instances. Precision and recall demonstrate effective attack detection with minimal false alarms or misses. The balanced F1-Score confirms reliable real-time IIoT threat defense.

TABLE I
Comparison of Performance Metrics

Metric	LSTM	Isolation Forest
Accuracy	0.9899	0.9774
Precision	0.8182	0.8022
Recall	0.9759	0.7300
F1-Score	0.8901	0.7644



_deviceId: 34

_attackType: DDoS

_severity: 78

0: uint256[]: 0

1: uint256[]: 34

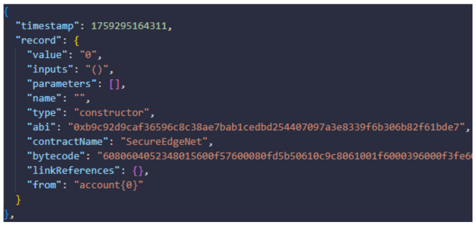
2: string[]: DDoS

3: uint8[]: 78

0: uint256: 1

Fig. 3. Querying IDS event logs from the Purechain

Figures 3 display retrieved blockchain logs from the contract, demonstrating recorded IDS alerts with event indices, timestamps, and attack types. Figure 4 shows the deployed SecureEdgeNet smart contract on the Purechain blockchain, including metadata and transaction details.



```
{
  "timestamp": 1759295164311,
  "record": {
    "value": "0",
    "inputs": "()",
    "parameters": [],
    "name": "",
    "type": "constructor",
    "abi": "0xb9c92d9caf36596c8c38ae7bab1cedbd254407097a3e8339f6b306b82f61bde7",
    "contractName": "SecureEdgeNet",
    "bytecode": "6080604052348015600f57600080fd5b50610c9c8061001f6000396000f3fe6
    "linkReferences": {},
    "from": "account{0}"
  }
},
```

Fig. 4. Smart contract deployment record on Purechain

These results show how SecureEdgeNet combines deep learning–based security analytics with blockchain logging. Purechain's lightweight PoA^2 consensus achieved sub-second transaction finality with negligible gas cost, ensuring throughput suitable for edge analytics. This integration strengthens data integrity and resilience against tampering and unauthorized access beyond standard federated methods.

IV. Conclusion

This study introduces SecureEdgeNet, an integrated edge security framework unifying Purechain-blockchain with LSTM-based IDS for robust IIoT cyber defense. The system excels in threat detection accuracy, data integrity, and operational scalability, making it well-suited for next-generation industrial networks. Future work includes extending quantum-resilient nodes and fully automated model lifecycle management over heterogeneous IIoT deployments.

V. Acknowledgment

This work was partly supported by the Innovative Human Resource Development for Local Intellectualisation program through the IITP grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 33%) and by Priority Research Centres 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] B. Alotaibi, "A survey on industrial internet of things security: Requirements, attacks, ai-based solutions, and edge computing opportunities," *Sensors*, vol. 23, no. 17, p. 7470, 2023.

[2] C. I. Okafor, L. A. C. Ahakonye, J. M. Lee, and D.-S. Kim, "Purequantum: Towards a scalable blockchain channel security in iot networks," *Blockchain: Research and Applications*, p. 100372, 2025.

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

[4] S. Selvarajan, G. Srivastava, A. O. Khadidos, A. O. Khadidos, M. Baza, A. Alshehri, and J. C.-W. Lin, "An artificial intelligence lightweight blockchain security model for security and privacy in iiot systems," *Journal of Cloud Computing*, vol. 12, no. 1, p. 38, 2023.

[5] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of blockchain in iot cybersecurity," *Sensors*, vol. 24, no. 10, p. 3111, 2024.

[6] 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.

[7] C. Djidjev, "siforest: Detecting network anomalies with set-structured isolation forest," in *2025 IEEE 4th International Conference on Computing and Machine Intelligence (ICMI)*. IEEE, 2025, pp. 1–5.