International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 2 (2025)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 2, 2025

Research Paper

Block Hunter Federated Learning For Cyber Threat Hunting In Block Chain Based IIOT Networks

[1] BUSHRA MUNEEB, [2] K. SWETHA, [3] M. SREEJA, [4] B. SHARADHA, [5] K. MAMATHA, [6] P. KEZIYA

[1] Assistant Professor, Department of Computer Science and Cyber Security, Princeton Institute of Engineering & Technology for Women, Hyderabad, India

[2,3,4,5,6] B. Tech Students, Department of Computer Science and Cyber Security, Princeton Institute of Engineering & Technology for Women, Hyderabad, India

Abstract:

Nowadays, blockchain-based technologies are being developed in various industries to improve data security. In the context of the Industrial Internet of Things (IIoT), a chain-based network is one of the most notable applications of blockchain technology. IIoT devices have become increasingly prevalent in our digital world, especially in support of developing smart factories. Although blockchain is a powerful tool, it is vulnerable to cyberattacks. Detecting anomalies in blockchain-based IIoT networks in smart factories is crucial in protecting networks and systems from unexpected attacks. In this article, we use federated learning to build a threat hunting framework called block hunter to automatically hunt for attacks in blockchain-based IIoT networks. Block hunter utilizes a cluster-based architecture for anomaly detection combined with several machine learning models in a federated environment. To the best of our knowledge, block hunter is the first federated threat hunting model in IIoT networks that identifies anomalous behavior while preserving privacy. Our results prove the efficiency of the block hunter in detecting anomalous activities with high accuracy and minimum required bandwidth.

Received: 02-5-2025 Accepted: 09-6-2025 Published: 18-6-2025

I.INTRODUCTION

In the era of the Fourth Industrial Revolution (Industry 4.0), Industrial Internet of Things (IIoT) is revolutionizing how manufacturing and automation processes operate by connecting devices, sensors, and systems to optimize industrial efficiency. However, this interconnectedness significantly increases the attack surface for cyber threats. With critical infrastructures being increasingly digitized, ensuring data integrity, security, and real-time threat detection in IIoT environments is of paramount importance. Blockchain

technology has emerged as a promising solution to secure IIoT ecosystems through decentralized, tamper-proof, and auditable ledgers. However, traditional machine learning-based threat detection systems are often centralized, vulnerable to data leakage, and unscalable in highly distributed IIoT architectures. This is where Federated Learning (FL) comes in—a privacy-preserving distributed machine learning paradigm that allows edge devices to collaboratively learn a shared model without sharing raw data.

This research introduces "Block Hunter", an intelligent federated learning-based cyber threat hunting framework designed specifically for blockchain-enabled IIoT networks. By combining blockchain for trust and traceability with federated deep learning for distributed threat detection, Block Hunter aims to achieve scalable, secure, and privacy-preserving cyber threat intelligence across industrial networks.

II.LITERATURE SURVEY

Significant progress has been made in both blockchain for IIoT security and federated learning for cybersecurity in recent years. Lin et al. (2017) explored the integration of blockchain into industrial networks, emphasizing its immutability and decentralized control for device authentication. Similarly, Ali et al. (2021) proposed a lightweight blockchain protocol tailored for resource-constrained IIoT devices.

In parallel, researchers have explored federated learning (FL) in the context of threat detection. McMahan et al. (2017) first introduced the concept of FL, followed by numerous implementations in healthcare, finance, and cybersecurity. Hardy et al. (2019) demonstrated privacy-preserving anomaly detection using FL in network intrusion systems. However, FL's vulnerability to poisoning attacks and lack of trust among edge nodes is a major concern.

To mitigate this, recent works have proposed blockchain-integrated FL frameworks. Kang et al. (2020) introduced a blockchain-based aggregation scheme for FL, ensuring traceable model updates. Liu et al. (2021) designed a secure FL system for vehicular networks using smart contracts for update verification. However, most existing systems still lack intelligent orchestration of threat intelligence, resource-aware model scheduling, and federated threat hunting optimized for IIoT environments.

III.EXISTING SYSTEM

Traditional cybersecurity systems in IIoT networks rely on centralized intrusion

detection systems (IDS) or cloud-based security monitoring platforms. These approaches have several drawbacks:

Single Point of Failure: If the central server is compromised, the entire system is vulnerable.

Latency: Centralized systems introduce delay in detecting fast-moving threats across distributed IIoT devices.

Privacy Concerns: Transmitting raw device data to central servers can violate privacy policies and regulations.

Incompatibility with Blockchain: Existing ML-based IDS do not natively integrate with blockchain infrastructures, leading to fragmented security frameworks.

Moreover, these systems often fail to dynamically adapt to zero-day attacks, collaboratively learn from distributed data, and verify the integrity of security model updates in a tamper-proof manner.

IV.PROPOSED SYSTEM

The proposed system, Block Hunter, is a novel federated learning-based framework for cyber threat hunting in blockchain-enabled IIoT networks. It consists of the following core components:

Federated Learning Nodes (FLNs): Distributed IIoT devices or edge gateways locally train lightweight anomaly detection models using device-specific data and periodically share model updates—not raw data—with a global aggregator.

Blockchain Layer: A private or consortium blockchain is used to record, validate, and timestamp model updates using smart contracts. This ensures traceability, tamper-resistance, and trust in the federated learning process.

Threat Intelligence Engine: A centralized yet privacy-preserving engine aggregates global models, performs threat correlation, and shares actionable intelligence (e.g., malicious IPs, anomalous patterns) with FLNs.

Attack Simulation & Feedback Loop: The system includes a sandboxed cyber-range to simulate ransomware, DDoS, or data exfiltration attacks and validate the accuracy of the federated models, further refining them.

Smart Contract-Driven Model Governance: Blockchain-based contracts enforce fair model contribution, reward mechanisms, and ensure accountability and auditability of updates.

By leveraging federated deep learning, smart contracts, and distributed ledger technology, the Block Hunter system enables IIoT environments to autonomously and collaboratively hunt cyber threats without sacrificing performance or privacy.

V.SYSTEM ARCHITECTURE

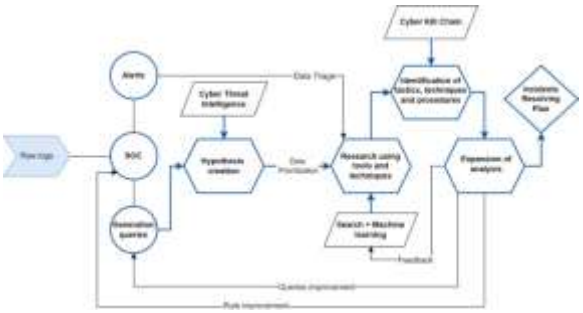

Fig 5.1 System Architecture

The diagram depicts an end-to-end cyber-threat-hunting workflow that transforms raw security logs into actionable incident-response plans through an iterative, intelligence-driven process. Raw log streams first arrive in the Security Operations Center (SOC), where analysts run detection queries that generate initial alerts; both the queries themselves and the resulting alerts feed a feedback loop that continually sharpens detection rules. Alerts are enriched with external and internal cyber-threat-intelligence feeds, enabling analysts to formulate investigative hypotheses. After a rapid triage step prioritizes the most critical hypotheses, selected data move into a research phase that leverages advanced tools, manual trade-craft, and machine-learning–powered search to expose hidden patterns and previously unknown threats. Findings are mapped to the Cyber Kill Chain, allowing analysts to pinpoint an adversary's tactics, techniques, and procedures (TTPs) and to understand where the attack currently sits in its lifecycle. Insights gained at this stage drive an expanded analysis of related assets and lateral-movement indicators, culminating in a comprehensive incident-resolution plan that covers containment, eradication, and recovery. Throughout the process, lessons learned—both from machine-learning feedback and from human analysis—loop back to refine SOC queries and detection rules, creating a virtuous cycle that continuously improves the organization's defensive posture against sophisticated, evolving cyber threats.

VI.IMPLEMENTATION

Fig 6.1 User Login

Fig 6.2 User Register

Fig 6.3 Enter Data

Fig 6.4 Admin Login

Fig 6.5 Add Categories

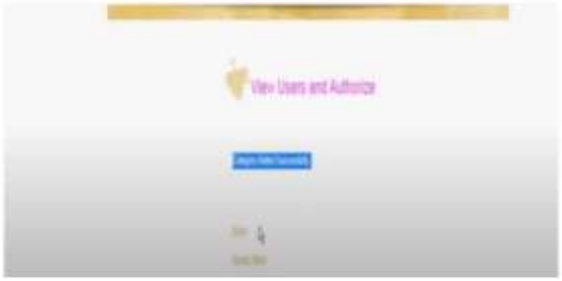

Fig 6.6 View Users And Authors

VII.CONCLUSION

Block Hunter presents an innovative paradigm for secure, distributed, and collaborative cyber threat hunting in blockchain-based IIoT networks. By uniting federated learning's data privacy and edge intelligence with blockchain's immutability and decentralized trust, this framework addresses the limitations of both standalone technologies. It enables real-time anomaly detection, secure model exchange, and verifiable audit trails for all updates and decisions.

This system not only enhances threat visibility across distributed IIoT devices but also mitigates data leakage risks, bottlenecks in centralized systems, and security model tampering. With increased industrial reliance on connected devices, such a hybrid framework ensures the resilience and robustness of critical infrastructure against advanced persistent threats (APTs).

VIII.FUTURE SCOPE

Block Hunter can be extended and improved in several ways:

- Integration with Zero Trust Architecture for enhanced access control at the device level.
- Use of differential privacy and homomorphic encryption to protect gradient information during model updates.

- Energy-aware FL scheduling algorithms for IIoT devices with limited computational resources.
- Application of GAN-based threat simulation to augment training data and improve model robustness.
- Use of cross-chain federated learning across multiple blockchain platforms.
- Incorporating Swarm Intelligence and Reinforcement Learning for autonomous threat response.
- Deployment as a cloud-native microservice framework for enterprise-wide security orchestration.

As IIoT deployments continue to scale across sectors like energy, transportation, and healthcare, Block Hunter can evolve into a next-generation AI-driven cyber defense layer, capable of detecting, analyzing, and mitigating complex cyberattacks in real time.

IX.REFERENCES

1. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. In AISTATS.
2. Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. IJ Network Security, 19(5), 653-659.
3. Ali, A., Anwar, F., & Haseeb, K. (2021). Lightweight blockchain for IIoT security: Survey and framework proposal. IEEE Access, 9, 57853-57877.
4. Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., & Hossain, E. (2020). Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal, 6(3), 4660–4670.
5. Hardy, S., Chen, W. M., Smith, N., & Mackey, L. (2019). Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption. arXiv:1711.10677.
6. Liu, Y., Li, J., Zhang, T., Tang, M., & Yu, W. (2021). Blockchain-based federated learning for secure data sharing in vehicular networks. Future Generation Computer Systems, 113, 175–186.

7. Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2019). Machine learning in IoT security: Current solutions and future challenges. IEEE Communications Surveys & Tutorials, 22(3), 1686-1721.
8. Feng, J., Zhang, S., He, L., & Liu, Y. (2020). SecFL: A secure federated learning framework for industrial internet of things. Computers & Security, 103, 102162.
9. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303.
10. Zhang, C., Yang, Q. (2021). A survey on federated learning. IEEE Transactions on Knowledge and Data Engineering, 34(5), 2346-2367.