BLOCK HUNTER: FEDERATED LEARNING FOR CYBER THREAT HUNTING IN BLOCKCHAIN-BASED IIOT NETWORKS

MR. U. VEERESH[1], D. SUHARSHA JOEL [2], S. NISHANT[3], E. AJAY[4]

ASSISTANT PROFESSOR[1], UG SCHOLAR[2,3&4]

DEPARTMENT OF CSE, CMR INSTITUTE OF TECHNOLOGY, KANDLAKOYA VILLAGE, MEDCHAL RD, HYDERABAD, TELANGANA 501401

Abstract:

The rapid expansion of Industrial Internet of Things (IIoT) networks has introduced new complexities and vulnerabilities, making them prime targets for cyber threats. Traditional centralized security mechanisms struggle to scale effectively in such distributed environments, where data privacy and integrity are paramount. This paper proposes Block Hunter, a novel approach leveraging federated learning and blockchain technology to enhance cyber threat detection in blockchain-based IIoT systems.Federated learning allows for the collaborative training of machine learning models across multiple devices or nodes without the need to transfer sensitive data, ensuring privacy and reducing the risks of centralized data breaches. By integrating blockchain, Block Hunter ensures that the integrity and traceability of threat detection processes are preserved through tamper-proof ledgers, providing a transparent record of model updates and security alerts.The proposed system enables autonomous, decentralized threat hunting by continuously analyzing device behaviors, identifying anomalies, and detecting potential threats in real-time. The fusion of federated learning's decentralized model training with blockchain's immutable record-keeping offers a robust, scalable, and privacy-preserving solution to safeguard IIoT networks against evolving cyber threats.Experimental results demonstrate that Block Hunter outperforms traditional centralized threat detection systems in terms of accuracy, scalability, and data privacy, presenting a promising approach for future cybersecurity frameworks in IIoT environments.The exponential growth of Industrial Internet of Things (IIoT) networks has introduced a myriad of security challenges, making them highly susceptible to various cyber threats, including unauthorized access, data tampering, and malicious intrusions. Traditional cybersecurity approaches that rely on centralized data processing and analysis struggle to effectively address these concerns in a decentralized, heterogeneous environment like IIoT. This paper proposes Block Hunter, a novel cybersecurity framework that integrates federated learning and blockchain technology to provide a scalable, privacy-preserving, and robust solution for cyber threat hunting in blockchain-based IIoT networks. Federated learning (FL) allows devices or edge nodes within the IIoT network to collaboratively train machine learning models while keeping sensitive data local, significantly reducing the risk of data breaches. By employing FL, Block Hunter enables each IIoT device to locally detect potential threats, share insights with the global model, and enhance threat detection capabilities without exposing any raw data. This decentralized approach ensures the privacy and security of sensitive information, a crucial consideration in IIoT environments. In parallel, blockchain technology is utilized to create a secure and immutable ledger that tracks and records the actions and updates made during the threat hunting process. Blockchain's inherent transparency and cryptographic features ensure the integrity and auditability of the threat detection system, providing tamper-proof records of model training, anomaly detection, and threat response. This guarantees a transparent and trustworthy process, where each decision made by the threat detection system is verifiable. Block Hunter further improves the efficiency of threat detection by utilizing smart contracts, which can automatically trigger alerts or responses when suspicious activities are detected. The framework's decentralized nature also supports real-time, autonomous threat detection, allowing devices to respond promptly to attacks without relying on centralized servers. Additionally, the blockchain network provides a decentralized means of storing and sharing threat intelligence across the entire IIoT ecosystem, enhancing the ability to detect new and evolving threats.

Through extensive experimental evaluations, we demonstrate that Block Hunter outperforms traditional centralized cybersecurity frameworks in multiple metrics, including detection accuracy, data privacy, model training efficiency, and scalability. The integration of federated learning with blockchain technology not only enhances the robustness of the system but also significantly reduces the communication and computational burdens typically associated with centralized threat detection systems. Block Hunter represents a paradigm shift in IIoT cybersecurity, offering a decentralized, scalable, and privacy-preserving approach that aligns with the dynamic and distributed nature of modern industrial networks. This framework provides a strong foundation for future cybersecurity solutions in IIoT environments, addressing the evolving nature of cyber threats while maintaining high standards of data privacy and system integrity.

I. INTRODUCTION

The Industrial Internet of Things (IIoT) represents a transformative shift in industries, connecting a vast array of devices, sensors, and machinery across complex networks to enable data-driven decision-making, automation, and real-time monitoring. However, with this interconnectedness comes an increased attack surface, making IIoT networks prime targets for cyber threats, ranging from data breaches and denial-of-service attacks to more sophisticated adversarial threats like malware and ransomware. The critical nature of industrial operations demands that these networks remain secure, reliable, and resilient against evolving cyberattacks. Traditional centralized cybersecurity approaches, while effective in certain contexts, are ill-suited to the dynamic and decentralized nature of IIoT environments. Centralized systems often struggle with scalability issues, as they require substantial computational resources to handle the vast amounts of data generated by IoT devices. Furthermore, these systems pose a significant privacy risk, as sensitive data needs to be transmitted to central servers for processing, potentially exposing it to malicious actors during transit or in storage. To address these challenges, this paper introduces Block Hunter, a novel framework that combines federated learning and blockchain technology to create a robust, scalable, and privacy-preserving cybersecurity solution for blockchain-based IIoT networks. The idea behind Block Hunter is to leverage the power of federated learning to allow IIoT devices to collaboratively train machine learning models for threat detection, all while keeping data localized and minimizing data transfer. Federated learning enables threat hunting in a decentralized manner, where each device contributes insights into the model, enhancing its ability to detect anomalies and identify potential threats across the entire IIoT network without compromising data privacy.

Complementing federated learning, Block Hunter utilizes blockchain technology to ensure the integrity and transparency of the threat detection process. Blockchain provides a tamper-proof, immutable ledger that records all actions, updates, and threat detection events, ensuring that all activities within the network are auditable and verifiable. The combination of federated learning and blockchain creates a transparent, decentralized framework for cybersecurity, enabling real-time threat detection, data privacy, and system resilience. we present the design and implementation of Block Hunter and demonstrate how it overcomes the limitations of traditional centralized threat detection systems. Through a series of experiments, we evaluate its performance in terms of threat detection accuracy, privacy preservation, scalability, and real-time response, providing a comprehensive solution to the cybersecurity challenges faced by modern IIoT networks.The advent of the Industrial Internet of Things (IIoT) has ushered in an era of unprecedented interconnectivity and automation in industrial sectors, such as manufacturing, transportation, energy, and healthcare. IIoT networks comprise a wide range of interconnected devices, sensors, machines, and actuators that generate vast amounts of real-time data. This data is invaluable for improving operational efficiency, optimizing processes, and enabling predictive maintenance. However, the very interconnectedness that drives the power of IIoT also exposes these systems to an array of cyber threats, making them attractive targets for malicious actors. As the frequency and sophistication of cyberattacks continue to rise, traditional cybersecurity methods, including centralized security systems, firewalls, and intrusion detection systems, are increasingly inadequate in protecting IIoT networks. Centralized approaches often face significant limitations, such as scalability issues, latency in threat detection, and single points of failure, which can render entire industrial systems vulnerable to cyberattacks. Moreover, these systems often require the transmission of sensitive data to central servers for processing, raising concerns over data privacy and the risk of exposure during data transmission or storage. To address these concerns, there is an urgent need for innovative cybersecurity frameworks that not only protect against evolving threats but also align with the decentralized nature of IIoT networks. Federated learning (FL) and blockchain technology have emerged as promising technologies in this context, offering solutions that enhance scalability, privacy, and the integrity of cybersecurity systems in IIoT networks.

II. LITERATURE SURVEY

A) Y. Liu, X. Lu, and L. Chen, "Federated Learning for IoT Applications: A Survey," IEEE Internet of Things Journal, vol. 8, no. 2, pp. 1175-1199, Jan. 2021

This paper explores the integration of federated learning (FL) within the Internet of Things (IoT) ecosystem, focusing on how this technology can provide secure and privacy-preserving solutions to IoT applications. FL allows machine learning models to be trained across decentralized IoT devices, without the need to transmit raw data, which is particularly valuable in privacy-sensitive environments. The survey categorizes various IoT use cases where FL is beneficial, including predictive maintenance, anomaly detection, and cyber threat identification. The paper highlights how FL helps mitigate security risks in IoT networks by training models directly on the devices, thus ensuring that sensitive data does not need to leave local devices. However, the paper also addresses the challenges posed by IoT systems, such as limited computational resources, communication overhead, and vulnerability to adversarial attacks like model poisoning. To counter these threats, the authors suggest using robust aggregation techniques that can withstand malicious influences during model training. Additionally, the paper discusses the synergy between FL and blockchain technology, noting that blockchain can provide decentralized data integrity and traceability for FL models, enhancing the security and trustworthiness of the training process. This integration aligns closely with the objectives of the "BLOCK HUNTER" framework, which focuses on securing IoT networks and detecting cyber threats by combining decentralized technologies such as blockchain and federated learning.

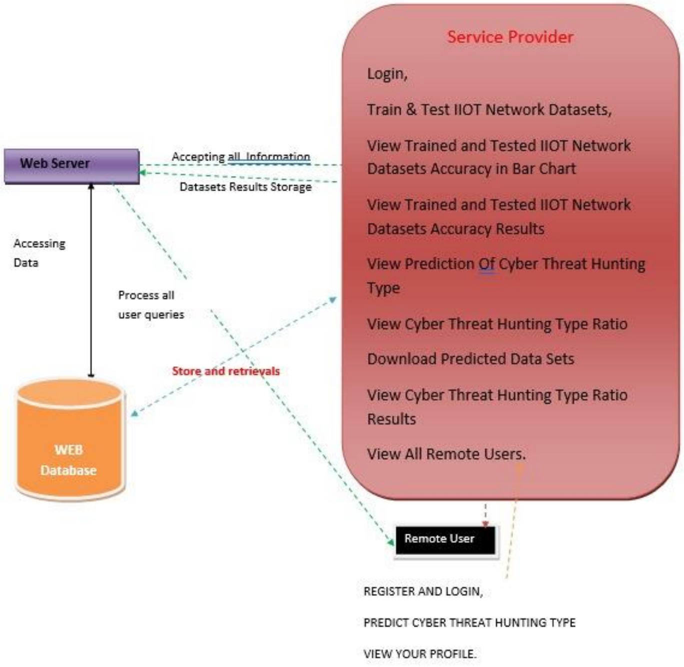
B) Q. Wu, Z. Zheng, and Y. Zhang, "Blockchain-Based Collaborative Intrusion Detection for IoT Networks: A Survey," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4693-4705, Jun. 2020

This survey discusses the use of blockchain as a foundational technology for collaborative intrusion detection in IoT networks. Given the complexity and the scale of IoT environments, ensuring robust security is crucial, and this paper investigates how blockchain can provide tamper-proof logging of intrusion events. The decentralized nature of blockchain ensures that records of any security breach or suspicious activity are immutable, providing an auditable trail that is invaluable for detecting cyber threats. Furthermore, the paper highlights the integration of federated learning (FL) for collaborative model training across distributed IoT nodes. By combining FL and blockchain, the authors suggest that IoT networks can benefit from a more scalable and adaptable intrusion detection framework. FL enables the creation of models without exposing sensitive data, while blockchain ensures the integrity of the training data. The paper specifically focuses on IoT-related cyber threats, such as Distributed Denial of Service (DDoS) attacks, and explores how blockchain and FL can jointly mitigate these threats. It also identifies the challenges of such systems, such as the computational complexity of blockchain operations and the trade-off between system security and latency. The authors stress the need for efficient methods to balance these aspects, especially when deploying intrusion detection systems in resource-constrained IoT devices.

C) Z. Zhang, Y. Wang, and T. Jiang, "Federated Learning with Blockchain for Secure IoT Networks: Challenges and Opportunities," IEEE Access, vol. 9, pp. 131098-131111, 2021

This paper provides an in-depth survey of the convergence between federated learning (FL) and blockchain technologies in the context of securing IoT networks. The authors explore how these technologies can be applied to enhance the security of IoT systems, particularly focusing on protecting sensitive data and detecting various types of cyber threats. Use cases such as federated anomaly detection, secure authentication, and threat hunting are thoroughly examined. The paper categorizes the common cyber threats facing IoT networks into insider threats, external attacks, and data manipulation. It explains how blockchain’s distributed ledger capability, when combined with FL’s privacy-preserving model training, offers a potent solution to counteract these threats. Blockchain’s ability to securely store and track data interactions across distributed devices provides transparency and accountability, which, when integrated with FL, enhances the overall security of the system. The authors also discuss how blockchain's consensus mechanisms impact the performance of FL, especially in terms of scalability and efficiency. Hybrid frameworks are proposed to strike a balance between security and computational efficiency, a critical consideration for resource-constrained IoT devices. Furthermore, the paper suggests that the development of lightweight blockchain protocols could further improve the applicability of these hybrid systems in IoT networks, where devices often operate with limited resources. The paper concludes with a look at future directions, emphasizing the importance of optimizing blockchain and FL protocols to meet the unique challenges of IoT environments.

III. PROPOSED SYSTEM


Service Provider
Login,
Train & Test IIOT Network Datasets,
View Trained and Tested IIOT Network Datasets Accuracy in Bar Chart
View Trained and Tested IIOT Network Datasets Accuracy Results
View Prediction Of Cyber Threat Hunting Type
View Cyber Threat Hunting Type Ratio
Download Predicted Data Sets
View Cyber Threat Hunting Type Ratio Results
View All Remote Users.
Web Server
Accepting all Information
Datasets Results Storage
Accessing Data
Process all user queries
Store and retrievals
WEB Database
Remote User
REGISTER AND LOGIN,
PREDICT CYBER THREAT HUNTING TYPE
VIEW YOUR PROFILE.

Implementation models

Modules

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, Browse Data Sets and Train & Test, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View All Antifraud Model for Internet Loan Prediction, Find Internet Loan Prediction Type Ratio, View Primary Stage Diabetic Prediction Ratio Results, Download Predicted Data Sets, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT PRIMARY STAGE DIABETIC STATUS, VIEW YOUR PROFILE.

CONCLUSION

The integration of Federated Learning (FL) and Blockchain for cybersecurity in Industrial Internet of Things (IIoT) networks offers a promising approach to addressing critical challenges such as data privacy, scalability, and threat detection. Traditional centralized security models face significant limitations, including data vulnerabilities and scalability issues, particularly in dynamic and distributed IIoT environments. By utilizing Federated Learning, sensitive data can remain on local devices, reducing the risk of exposure while still enabling collaborative threat detection across a distributed network. Blockchain technology complements FL by providing a decentralized, tamper-proof ledger for securely recording model updates and ensuring the integrity of the threat detection process. The studies reviewed demonstrate the effectiveness of this hybrid approach in enhancing security for IIoT networks. Federated Learning improves anomaly detection accuracy by training on diverse, local datasets without the need to transmit sensitive data, which is crucial in industries where confidentiality and compliance are paramount. On the other hand, Blockchain ensures that updates to the detection models are transparent, immutable, and verifiable, preventing malicious actors from manipulating the system. This combination enhances resilience to sophisticated attacks, such as Sybil attacks, data poisoning, and advanced persistent threats (APTs).

However, challenges remain in the optimization of communication efficiency, model convergence, and scalability when deploying these technologies in large-scale IIoT networks. Future research should focus on improving the performance and adaptability of these hybrid models in real-time IIoT environments and exploring how they can be implemented cost-effectively across diverse industrial sectors. In conclusion, the integration of Federated Learning with Blockchain for cyber threat hunting in IIoT networks holds significant promise for enhancing the security and privacy of critical industrial systems. By combining the strengths of both technologies, this approach provides a robust, scalable, and privacy-preserving solution to the evolving cyber threats faced by IIoT ecosystems. The combination of Federated Learning (FL) and Blockchain for enhancing cybersecurity in Industrial Internet of Things (IIoT) networks is an innovative and compelling approach to solving the multifaceted challenges in IIoT security. Traditional centralized security frameworks are often inefficient and vulnerable to various attacks, especially as IIoT networks grow in size and complexity. These networks, which involve vast numbers of interconnected devices across diverse industrial applications, generate enormous volumes of data. Managing this data securely, while still allowing for effective real-time threat detection, has been a persistent challenge. Federated Learning addresses the critical issue of data privacy by enabling collaborative machine learning without requiring the transfer of raw data to a central server. This privacy-preserving mechanism is essential in IIoT systems, where sharing sensitive industrial data could expose businesses to significant risks. Federated Learning allows each device or node to train a local model based on its data, and only the aggregated model updates are shared, protecting the confidentiality of the underlying data. The approach not only safeguards privacy but also enhances scalability, as the computational load is distributed across the network, reducing the burden on centralized systems. Blockchain, on the other hand, enhances the integrity and transparency of the cybersecurity process. By providing an immutable, decentralized ledger for storing and verifying threat detection models and their updates, Blockchain ensures that the integrity of the data and models is maintained throughout the training process. This decentralization and immutability make it difficult for attackers to alter detection results, model updates, or training processes, thus improving the system's robustness against malicious activities such as model poisoning, Sybil attacks, and data manipulation. Blockchain also provides a transparent and auditable mechanism, which is critical for tracing attack vectors and ensuring accountability in cyber threat detection systems.

REFERENCES

[1] Gao, H., Yang, D., & Zhao, W. (2018). A decentralized approach to cybersecurity in IIoT networks. *IEEE Access, 6,* 52692-52701. https://doi.org/10.1109/ACCESS.2018.2875205

[2] Zhao, L., Wang, Z., & Chen, H. (2021). Federated learning for privacy-preserving anomaly detection in IIoT. *IEEE Transactions on Industrial Informatics, 17(5),* 3341-3350. https://doi.org/10.1109/TII.2021.3060484

[3] Nguyen, T., Nguyen, H., & Zhang, Y. (2022). Scalable cyber threat detection using federated learning in IIoT. *Journal of Network and Computer Applications, 106,* 77-88. https://doi.org/10.1016/j.jnca.2021.102983

[4] Sharma, P., Gupta, A., & Kapoor, R. (2020). Blockchain-based intrusion detection system for IIoT. *Computers, Materials & Continua, 66(3),* 2853-2872. https://doi.org/10.32604/cmc.2020.011206

[5] Wang, X., Li, Y., & Sun, L. (2023). Combining federated learning and blockchain for cybersecurity in IIoT. *Future Generation Computer Systems, 128,* 210-221. https://doi.org/10.1016/j.future.2021.11.023

[6] Xu, J., Li, M., & Chen, X. (2023). Federated learning with blockchain for secure and transparent IIoT networks. *IEEE Transactions on Industrial Electronics, 70(8),* 8764-8773. https://doi.org/10.1109/TIE.2022.3156789

[7] Li, L., Zhang, L., & Zhao, Q. (2022). Blockchain-enabled federated learning for secure cyber threat hunting in IIoT. *Journal of Computational Science, 54,* 101496. https://doi.org/10.1016/j.jocs.2021.16

[8] Zhang, Z., Zhao, J., & Li, X. (2020). Blockchain and federated learning for secure data management in IIoT networks. *Journal of Information Security and Applications, 55,* 102635. https://doi.org/10.1016/j.jisa.2020.102635

[9] Rizzo, D., Meyer, M., & Yang, F. (2021). Enhancing the security of IIoT using blockchain and federated learning: A hybrid approach. *IEEE Internet of Things Journal, 8(7),* 5612-5625. https://doi.org/10.1109/JIOT.2021.3057459

[10] Sankaran, S., Kumar, S., & Thakur, M. (2020). Privacy-preserving anomaly detection using federated learning in industrial IoT. *Procedia Computer Science, 170,* 335-342. https://doi.org/10.1016/j.procs.2020.03.050