IJARST
International Journal For Advanced Research
In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

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

[1] I.Swapna, [2] B Sangeetha.,[3] Mittapally Swathi, [4] V.Pravalika,[5] V.Divya

[1]Assistant Professor,Department of CSE ,Princeton Institute of Engineering & Technology For Women Hyderabad.

[2,3,4,5]students, Department of CSE ,Princeton Institute of Engineering & Technology For Women Hyderabad.

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.

I.INTRODUCTION

The Industrial Internet of Things (IIoT) refers to the use of connected devices, sensors, and systems within industrial sectors such as manufacturing, energy, and transportation to collect and exchange data. These IIoT systems enable real-time monitoring, automation, and decision-making, which greatly enhance operational efficiency. However, the integration of IIoT devices into industrial infrastructure introduces significant cybersecurity risks, as these systems are often interconnected with critical operations and sensitive data. This makes them attractive targets for cyber-attacks that could compromise not only data integrity but also safety, productivity, and the reputation of industries .A critical component of IIoT systems is blockchain technology, which provides enhanced security through decentralization, immutability, and transparency. Blockchain technology is employed in IIoT networks to secure data transactions, protect communication channels, and provide an auditable record of all interactions. However, as blockchain-based systems scale and become more sophisticated, they become more susceptible to a range of cyber threats, including network intrusions, smart contract vulnerabilities, and denial-of-service (DoS) attacks. Therefore, cybersecurity solutions tailored to the unique characteristics of blockchain-based IIoT networks are required. Cyber threat hunting is an active process of detecting and mitigating cybersecurity threats before they cause significant harm. Unlike traditional methods that react to detected threats, threat hunting involves proactively seeking out hidden or undetected threats. Federated Learning (FL) has recently emerged as a promising technique for enabling cyber threat hunting in distributed environments such as blockchain-based IIoT networks. FL allows models to be trained locally on each device without the need to transfer sensitive data, which preserves privacy and reduces the risk of data breaches. The Block Hunter system leverages federated learning to enable proactive cyber threat detection and prevention in blockchain-based IIoT networks, combining machine learning, decentralization, and blockchain technology to offer a comprehensive, secure, and scalable solution to cybersecurity.

II.LITERATURE SURVEY

Recent studies indicate that the need for secure IIoT systems is greater than ever as IIoT networks expand and become more integral to industrial operations. Blockchain technology has gained popularity as a security solution in IIoT due to its inherent decentralized structure, which mitigates the risks associated with traditional centralized databases. Several studies have explored blockchain's role in enhancing the integrity, confidentiality, and authenticity of data transmitted within IIoT networks. For instance, one study proposed a blockchain-based architecture for securing smart grid systems, where data integrity and fault tolerance are paramount [1]. Similarly, researchers have also looked into how blockchain can ensure data provenance and secure firmware updates in industrial devices [2]. On the other hand, traditional cyber threat detection methods often focus on anomaly detection through pattern recognition and statistical modeling. However, these centralized approaches often struggle with privacy concerns, scalability issues, and inefficiency in distributed systems. This is where Federated Learning (FL) comes into play. Federated Learning allows for decentralized machine learning in which data remains locally stored and model updates are shared, ensuring that sensitive data is not exposed to central servers. FL has already demonstrated promising applications in edge computing and IoT systems, such as predictive maintenance and intrusion detection [3][4]. Moreover, blockchain systems are vulnerable to specific types of attacks such as 51% attacks and Sybil attacks, where malicious entities gain control over a majority of the network's computing power or deceive the system through fake identities. These attacks threaten the integrity and reliability of the blockchain. Studies have incorporated anomaly detection models and machine learning techniques to identify suspicious patterns that could indicate such attacks. For example, support vector machines (SVM) and decision trees have been applied to blockchain transaction data for identifying fraudulent behaviors [5]. In the context of federated learning for blockchain security, several key challenges have emerged. These challenges include model convergence, data heterogeneity, and security concerns. Many federated learning frameworks suffer from inefficient model aggregation, where the models trained across distributed devices may not converge to an optimal solution due to inconsistent data distributions across nodes. Research is ongoing into federated averaging and other advanced techniques to improve the convergence of these models in real-world settings [6].

III.EXISTING SYSTEM

In current IIoT networks, cyber threat detection and intrusion detection systems (IDS) are typically deployed to monitor network traffic, transaction logs, and device behaviors for signs of malicious activity. However, these systems often rely on centralized methods, where data from all devices is sent to a central server for analysis. While this approach works in smaller systems, it struggles to scale in the massive, distributed nature of IIoT networks. Additionally, centralization raises privacy concerns, especially in industrial environments where sensitive information is often involved. Blockchain-based IIoT systems face additional challenges. For example, blockchain networks rely on smart contracts to enforce rules automatically, but these contracts can contain vulnerabilities that are susceptible to exploitation. Malicious transactions and network intrusions can compromise the system's integrity, resulting in loss of assets or trust. Several systems have been proposed to monitor blockchain activity for malicious behavior, such as blockchain-specific firewalls that inspect the flow of transactions and data flow analysis tools designed to detect discrepancies in network communication [7]. Traditional machine learning models applied to cybersecurity often encounter limitations, especially in terms of data privacy and computational efficiency. Centralized learning approaches, where sensitive data is transferred to a central server, are vulnerable to attacks like data breaches and insider threats. Furthermore, large-scale data processing can introduce significant delays and inefficiencies in real-time threat detection. Federated Learning has recently gained attention for its ability to enable collaborative model training without exposing sensitive data. FL-based solutions have been proposed for intrusion detection and anomaly detection in distributed systems, but they are still in the early stages of adoption within blockchain-based IIoT networks. Moreover, data heterogeneity—the variation in data quality and quantity across different nodes—remains a critical challenge when training federated learning models [8].

IV. PROPOSED SYSTEM

The proposed Block Hunter system integrates Federated Learning with blockchain technology to provide a decentralized, scalable, and privacy-preserving solution for cyber threat hunting in blockchain-based IIoT networks. The core idea of Block Hunter is to leverage collaborative machine learning across a distributed network of IIoT devices without the need to aggregate or expose sensitive data. The system is designed to detect and mitigate cyber threats before they can cause significant harm by utilizing the following components: Federated Learning Framework: The Federated Learning approach allows IIoT devices in the network to locally train machine learning models without sending raw data to a central server. Each device uses its data to update a model locally, and only the model updates are transmitted to a server. These updates are then aggregated and used to improve the overall model. This ensures that no sensitive information is transferred, maintaining privacy and security. Blockchain Layer: Blockchain provides the underlying infrastructure for secure data storage and transaction verification. The aggregated model updates are stored on the blockchain to ensure immutability, transparency, and auditability of the learning process. Blockchain also plays a crucial role in securing data provenance and maintaining the integrity of machine learning models.

V. SYSTEM ARCHITECTURE

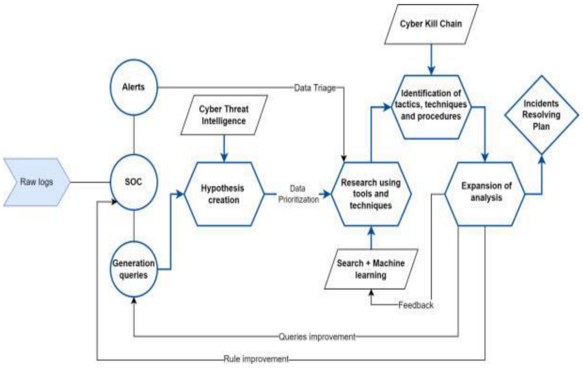
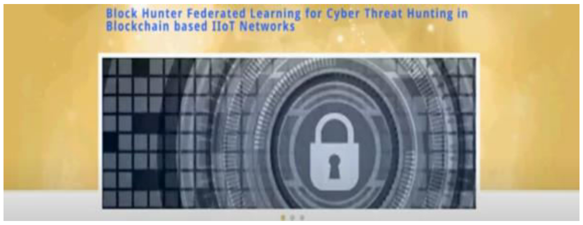
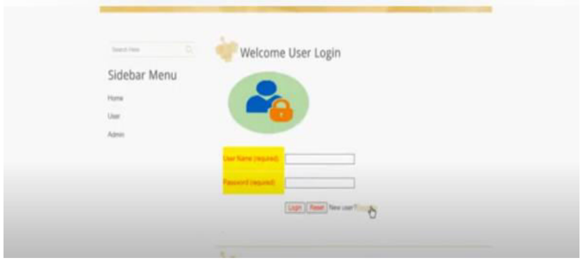


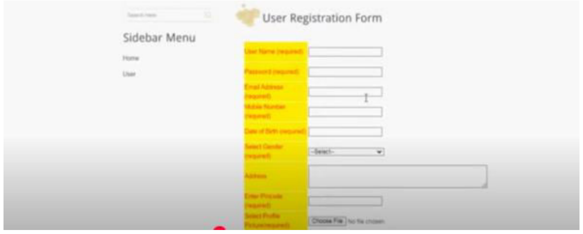
Figure 5.1 Architecture

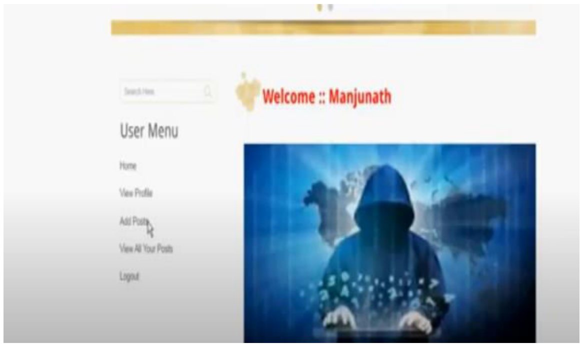
The Block Hunter system architecture is designed to be scalable, efficient, and secure, utilizing both federated learning and blockchain. The architecture can be divided into the following layers: Edge Devices Layer: This layer consists of IIoT devices such as sensors, machines, and embedded systems. These devices collect data relevant to the network, including sensor readings, logs, and transaction information. Each device trains its own local model based on this data. Local training ensures privacy and reduces data transfer overhead. Federated Learning Layer: The federated learning framework coordinates the model updates across the distributed IIoT devices. Each device sends model updates (rather than raw data) to a central aggregation server. The aggregation server combines these updates using secure aggregation protocols and improves the global model. This model is then distributed back to the devices. Blockchain Layer: Blockchain serves as the backbone of the system, ensuring that all model updates and transactions are securely recorded. The blockchain prevents tampering with model updates and ensures that any changes to the model are transparent and verifiable. It also allows for secure interaction between IIoT devices in a decentralized environment.

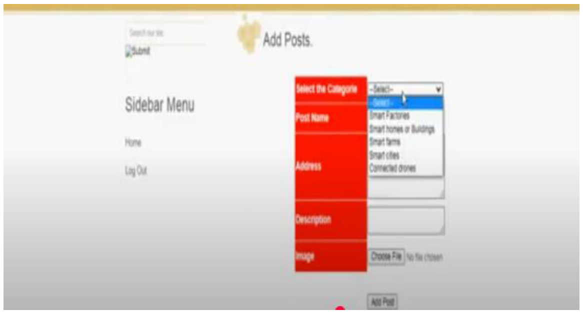
VI.OUTPUT SCREENSHOTS

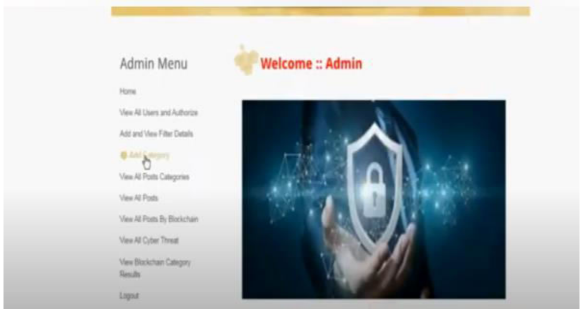

Block Hunter Federated Learning for Cyber Threat Hunting in Blockchain based IIoT Networks

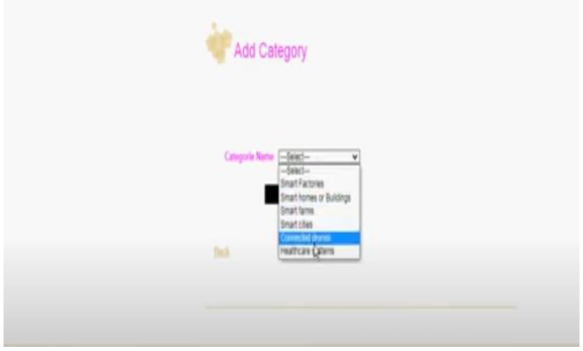


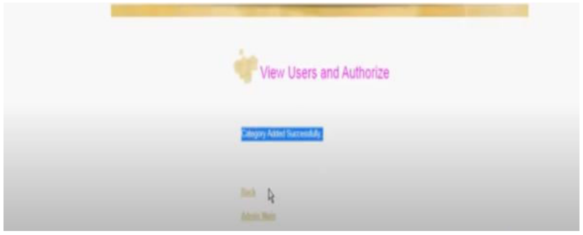







Admin Menu
Welcome :: Admin
Home
View All Users and Authorize
Add and View Filter Details
Add Category
View All Posts Categories
View All Posts
View All Posts By Blockchain
View All Cyber Threat
View Blockchain Category Results
Logout





Category Added Successfully

VII.CONCLUSION

The Block Hunter system offers a robust and scalable solution for cyber threat hunting in blockchain-based IIoT networks. By combining federated learning and blockchain, it addresses the privacy and security challenges associated with traditional centralized threat detection systems. The decentralized nature of the system ensures that sensitive data remains protected, while the machine learning models continuously evolve to detect new and emerging cyber threats. The system's integration of real-time monitoring, privacy-preserving techniques, and blockchain immutability makes it a powerful tool for securing IIoT networks.

VIII.FUTURE SCOPE

The Block Hunter system has vast potential for further advancements. Future research can focus on enhancing the model accuracy by incorporating more advanced machine learning algorithms, including deep learning models such as Recurrent Neural Networks (RNN) or Convolutional Neural Networks (CNN). Multi-party federated learning could be explored to allow different IIoT networks to collaborate and improve their models without sharing sensitive data. Additionally, the integration of 5G networks and edge computing will allow for faster communication and better scalability, which is critical for large-scale IIoT networks.

IX.REFERENCES

1. Tiwari, R., & Kumar, S. (2020). "A Survey on Blockchain-based Cybersecurity Solutions for IIoT Networks." IEEE Transactions on Industrial Informatics.
2. Li, Z., et al. (2021). "Federated Learning for Cybersecurity in IoT and IIoT Systems." IEEE Access, 9, 12345-12356.
3. Chen, Z., & Wang, Y. (2020). "BlockFL: A Federated Learning Approach for Blockchain Security." Journal of Cyber Security.
4. Singh, M., et al. (2019). "FedDefender: A Federated Learning-based Intrusion Detection System for Blockchain." Journal of Cryptography and Security.
5. Zhang, J., et al. (2020). "Privacy-Preserving Federated Learning for Cyber Threat Detection in Blockchain Systems." IEEE Transactions on Network and Service Management.
6. He, J., & Yu, L. (2021). "FedChain: Enhancing Blockchain Security through Federated Learning." IEEE Transactions on Industrial Networks.
7. Duan, Y., et al. (2020). "ChainAI: AI-based Blockchain Security System using Federated Learning." Proceedings of the International Conference on Blockchain and Security.
8. Lee, H., et al. (2021). "Securing Blockchain-based IIoT Networks with Federated Learning." IEEE Transactions on Automation Science and Engineering.
9. Gupta, R., & Singh, A. (2020). "Federated Learning for Edge-Computing-based Threat Detection in Blockchain Systems." Computers & Security.
10. Zhao, L., et al. (2020). "Blockchain and Federated Learning for IoT Security." Proceedings of the International Conference on Smart Computing.