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

Mrs. K. Jhansi rani & mr. K. Mahendra[1],gunda naveen[2],vuppala sai sharan[3],vemula bhavya sri[4],muppidi sriman[5],galenka manas babu[6],t nikhitha[7]

[1]Assistant professor,department of information technology,malla reddy institute of engineering and technology(autonomous),dhulapally,secundrabad

[2,3,4,5,6,7]UG Students,department of information technology,malla reddy institute of engineering and technology(autonomous),dhulapally,secundrabad

ABSTRACT

The "Block Hunter: Federated Learning for Cyber Threat Hunting in Blockchain-Based IIoT Networks" project represents an innovative solution to the escalating challenges of cybersecurity in Industrial Internet of Things (IIoT) networks leveraging blockchain technology. In the interconnected landscape of IIoT, ensuring the security and integrity of data is paramount. This project introduces Block Hunter, a federated learning-based system designed to proactively identify and mitigate cyber threats within blockchain-based IIoT networks. Block Hunter capitalizes on the principles of federated learning, allowing edge devices within IIoT networks to collaboratively train machine learning models without sharing sensitive data. This decentralized approach enhances the resilience of the system against potential cyber threats by fostering collective intelligence without compromising individual data privacy.

The project encompasses key modules such as blockchain integration for secure and transparent data management, federated learning algorithms for collaborative threat detection, and a real-time threat response mechanism. The system continuously evolves its threat detection capabilities by aggregating insights from distributed edge devices, adapting to emerging cyber threats, and enhancing the overall cybersecurity posture of the IIoT network. By combining blockchain's inherent security features with federated learning's decentralized learning paradigm, Block Hunter offers a robust and scalable solution for cyber threat hunting in IIoT networks. The proposed system not only addresses current cybersecurity challenges but also positions itself as a forward-looking approach to safeguarding the integrity and functionality of blockchain-based IIoT ecosystems in the face of evolving cyber threats.

I. INTRODUCTION

In the rapidly advancing domain of Industrial Internet of Things (IIoT), where seamless connectivity and data integrity are paramount, the convergence of blockchain technology and cybersecurity stands as a crucial frontier. The "Block Hunter: Federated Learning for Cyber Threat Hunting in Blockchain-Based IIoT Networks" project represents an innovative response to the escalating challenges posed by cyber threats in IIoT ecosystems. By combining the secure foundations of blockchain with the decentralized learning paradigm of federated learning, this project seeks to fortify IIoT networks against evolving cybersecurity threats.

As industries increasingly adopt IIoT networks for efficient data exchange and real-time monitoring, the vulnerabilities to cyber threats become more pronounced. Block Hunter aims to redefine the defense mechanisms in place by introducing a federated learning-based system that operates within the secure framework of blockchain. This unique amalgamation not only prioritizes the collective intelligence of edge devices within the IIoT network but also ensures the privacy and security of sensitive data.

The multifaceted approach of Block Hunter encompasses the integration of blockchain for transparent and secure data management, federated learning algorithms for decentralized threat detection, and a responsive mechanism to counteract identified threats in real-time. This project is poised to usher in a new era of cybersecurity resilience, where the collaborative strength of decentralized learning and the immutability of blockchain collectively contribute to safeguarding the integrity and functionality of IIoT networks.

As we delve into the intricacies of Block Hunter, we embark on a journey towards not just addressing current cybersecurity challenges but fostering an anticipatory and adaptive defense mechanism against the ever-evolving spectrum of cyber threats in blockchain-based IIoT environments.

II. LITERATURE REVIEW

1.**Block Hunter: Federated Learning for Cyber Threat Hunting in Blockchain-Based IIoT Networks,Abbas Yazdinejad; Ali Dehghantanha; Reza M. Parizi; Mohammad Hammoudeh; Hadis Karimipour,** 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.

III.EXISTING SYSTEM

In the existing landscape of Industrial Internet of Things (IIoT) cybersecurity, conventional approaches often rely on centralized security measures and signature-based detection systems. While these methods provide a level of protection, they face challenges in adapting to the dynamic nature of cyber threats, especially in distributed and interconnected IIoT networks. Moreover, traditional systems may encounter difficulties in ensuring data privacy, particularly when dealing with sensitive information from edge devices.

Disadvantages

- The system is not implemented the Isolation Forest (IF) model which falls under the Tree-based anomaly detection algorithms category.
- The system is not implemented Cluster-Based Local Outlier Factor.

IV.PROPOSED SYSTEM

The "Block Hunter: Federated Learning for Cyber Threat Hunting in Blockchain-Based IIoT Networks" project proposes a revolutionary shift from conventional cybersecurity approaches. The system introduces federated learning, a decentralized learning paradigm, within the secure framework of blockchain. This novel combination empowers edge

devices in IIoT networks to collaboratively train machine learning models without compromising the privacy of sensitive data. The proposed system encompasses modules such as blockchain integration, federated learning algorithms, real-time threat response, and adaptive learning mechanisms to proactively detect and counter cyber threats in IIoT environments.

- **Blockchain Integration Module:**

Ensures secure and transparent data management within the IIoT network, leveraging the immutability and cryptographic features of blockchain.

- **Federated Learning Algorithms Module:**

Employs machine learning models that operate in a decentralized manner, allowing edge devices to collaboratively train models while keeping sensitive data localized.

- **Real-Time Threat Response Module:**

Implements mechanisms to respond to identified threats in real-time, enabling immediate mitigation actions to safeguard the integrity of the IIoT network.

- **Adaptive Learning Mechanism Module:**

Allows the system to continuously adapt and evolve its threat detection capabilities based on insights gathered from distributed edge devices, ensuring resilience against emerging cyber threats.

Advantages

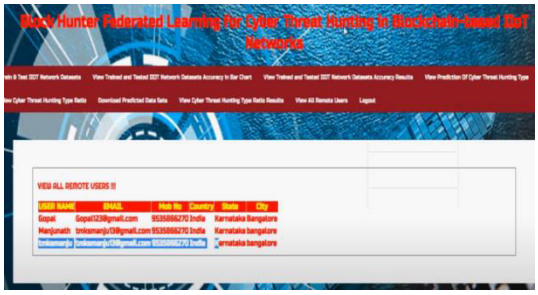
- Federation Construction: The subset of smart factory members, cluster, selected to receive the model locally.
- Decentralized Training: When a cluster of smart factories is selected, it updates its model using its local data.
- Model Accumulation: Responsible for accumulating and merging the data models. Data is not sent and integrated from the federation to the server individually.
- Model Aggregation (FedAvg): Parameter server aggregates model weights to compute an enhanced global model.

V.MODULES

1.Blockchain Integration Module:

This module focuses on integrating blockchain technology into the IIoT network. It includes components for secure and transparent data management, leveraging the immutability and

cryptographic features of blockchain to enhance data integrity.

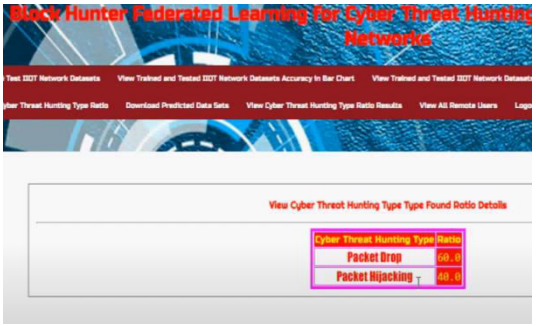


2.Federated Learning Algorithms Module:

The core of the system, this module involves the development and implementation of federated learning algorithms. These algorithms enable edge devices to collaboratively train machine learning models without sharing sensitive data. It includes mechanisms for model aggregation and update strategies.

3.Real-Time Threat Response Module:

This module is responsible for the real-time response to identified threats. It includes components for threat detection, alert generation, and automated or semi-automated responses to mitigate threats. Real-time response ensures a swift reaction to potential cyber threats.



4.Adaptive Learning Mechanism Module:

The adaptive learning module allows the system to continuously adapt and evolve its threat detection capabilities. It involves mechanisms for learning from the insights gathered from distributed edge devices, updating the federated learning models, and adjusting the system's threat detection strategies.

5.Secure Communication Module:

This module focuses on ensuring secure communication between edge devices, the IIoT network, and the blockchain. It includes encryption and authentication mechanisms to safeguard data transmission and maintain the privacy and integrity of communications.

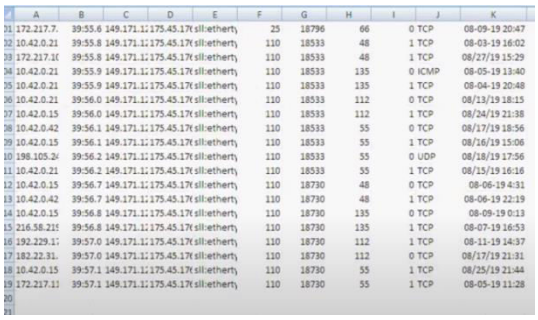
6.Decentralized Identity Management Module:

As part of ensuring the security and privacy of participants in the federated learning process, this module handles decentralized identity management. It

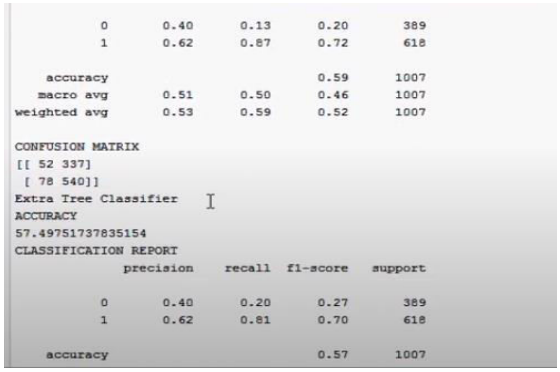
includes components for identity verification, access control, and maintaining the privacy of participants.

7.Data Privacy and Anonymization Module:

This module is crucial for ensuring data privacy in federated learning.



It involves techniques for anonymizing and encrypting data at the edge devices before sharing with the federated learning system, ensuring that sensitive information remains confidential.



```
              precision    recall  f1-score   support

           0       0.40      0.13      0.20       389
           1       0.62      0.87      0.72       618

    accuracy                           0.59      1007
   macro avg       0.51      0.50      0.46      1007
weighted avg       0.53      0.59      0.52      1007

CONFUSION MATRIX
[[ 52 337]
 [ 78 540]]
Extra Tree Classifier
ACCURACY
57.49751737835154
CLASSIFICATION REPORT
              precision    recall  f1-score   support

           0       0.40      0.20      0.27       389
           1       0.62      0.81      0.70       618

    accuracy                           0.57      1007
```

8.User Interface (UI) Module:

The UI module focuses on providing a user-friendly interface for system administrators and operators. It includes dashboards, visualization tools, and controls for monitoring the status of the federated learning process, threat alerts, and system performance.

VI.CONCLUSION

In conclusion, the "Block Hunter" project represents a paradigm shift in IIoT cybersecurity, introducing a decentralized and collaborative approach to threat hunting. By leveraging federated learning within a blockchain-based framework, the proposed system not only enhances the security posture of IIoT networks but also addresses challenges related to data privacy. The integration of blockchain ensures the integrity and transparency of data transactions, while federated learning empowers the network to collectively learn and adapt to evolving threats. With modules dedicated to blockchain integration, federated learning algorithms, real-time threat response, and adaptive learning mechanisms, Block Hunter offers a comprehensive solution for the dynamic cybersecurity landscape of blockchain-based IIoT networks. This project stands at the forefront of advancing security measures, ensuring the resilience and adaptability of IIoT ecosystems against emerging cyber threats.

VII.REFERENCES

1. J. Wan, J. Li, M. Imran, D. Li and F. e Amin, "A blockchain-based solution for enhancing security and privacy in smart factory", *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3652-3660, Jun. 2019.

2.F. Scicchitano, A. Liguori, M. Guarascio, E. Ritacco and G. Manco, "Blockchain attack discovery via anomaly detection", *Consiglio Nazionale delle Ricerche Istituto di Calcolo e Reti ad Alte Prestazioni*, 2019.

3.Q. Xu, Z. He, Z. Li, M. Xiao, R. S. M. Goh and Y. Li, "An effective blockchain-based decentralized application for smart building system management" in Real-Time Data Analytics for Large Scale Sensor Data, Amsterdam, The Netherlands:Elsevier, pp. 157-181, 2020.

4.B. Podgorelec, M. Turkanović and S. Karakatič, "A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection", *Sensors*, vol. 20, no. 1, 2020.

5.A. Quintal, "Veriblock foundation discloses mess vulnerability in ethereum classic blockchain", Jul. 2021, [online] Available: https://www.prnewswire.com/news-releases/veriblock-foundation-discloses-mess-vulnerability-in-ethereum-classic-blockchain-301327998.html.

6.M. Saad et al., "Exploring the attack surface of blockchain: A comprehensive survey", *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1977-2008, Jul.–Sep. 2020.

7.R. A. Sater and A. B. Hamza, "A federated learning approach to anomaly detection in smart buildings", *ACM Trans. Internet Things*, vol. 2, no. 4, Aug. 2021.

8.A. Yazdinejadna, R. M. Parizi, A. Dehghantanha and H. Karimipour, "Federated learning for drone authentication" in Ad Hoc Netw., vol. 120, 2021.

9.D. Preuveneers, V. Rimmer, I. Tsingenopoulos, J. Spooren, W. Joosen and E. Ilie-Zudor, "Chained anomaly detection models for federated learning: An intrusion detection case study", *Appl. Sci.*, vol. 8, no. 12, 2018.

10.L. Tan, H. Xiao, K. Yu, M. Aloqaily and Y. Jararweh, "A blockchain-empowered crowdsourcing system for 5G-enabled smart cities", *Comput. Standards Interfaces*, vol. 76, 2021.

11.L. Tseng, X. Yao, S. Otoum, M. Aloqaily and Y. Jararweh, "Blockchain-based database in an IoT environment: Challenges opportunities and analysis", *Cluster Comput.*, vol. 23, no. 3, pp. 2151-2165, 2020.

12.M. Signorini, M. Pontecorvi, W. Kanoun and R. Di Pietro, "BAD: A

blockchain anomaly detection solution", *IEEE Access*, vol. 8, pp. 173481-173490, 2020.

13.S. Iyer, S. Thakur, M. Dixit, R. Katkam, A. Agrawal and F. Kazi, "Blockchain and anomaly detection based monitoring system for enforcing wastewater reuse", *Proc. 10th Int. Conf. Comput. Commun. Netw. Technol.*, pp. 1-7, 2019.

14.S. Sayadi, S. B. Rejeb and Z. Choukair, "Anomaly detection model over blockchain electronic transactions", *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf.*, pp. 895-900, 2019.

15.Z. Il-Agure, B. Attallah and Y.-K. Chang, "The semantics of anomalies in IoT integrated blockchain network", *Proc. 6th HCT Inf. Technol. Trends*, pp. 144-146, 2019.

16.T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan and A.-R. Sadeghi, "DÏoT: A federated self-learning anomaly detection system for IoT", *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst.*, pp. 756-767, 2019.

17.H. Chai, S. Leng, Y. Chen and K. Zhang, "A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles", *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3975-3986, Jul. 2021.

18.M. Alazab, S. P. RM, P. M., P. K. R. Maddikunta, T. R. Gadekallu and Q.-V. Pham, "Federated learning for cybersecurity: Concepts challenges and future directions", *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3501-3509, May 2022.

19.H. B. McMahan, E. Moore, D. Ramage, S. Hampson and B. Agüera y Arcas, "Communication-efficient learning of deep networks from decentralized data", *Proc. 20th Int. Conf. Artif. Intell. Statist. ser. Proc. Mach. Learn. Res.*, pp. 1273-1282, 2017, [online] Available: https://proceedings.mlr.press/v54/mcmahan17a.html

20.N. Moussa and A. E. B. El Alaoui, "An energy-efficient cluster-based routing protocol using unequal clustering and improved ACO techniques for WSNs" in Peer-to-Peer Netw. Appl., vol. 14, pp. 1334-1347, 2021.

21.A. Yazdinejad, R. M. Parizi, G. Srivastava, A. Dehghantanha and K.-K. R. Choo, "Energy efficient decentralized authentication in internet of underwater things using blockchain", *Proc. IEEE Globecom Workshops*, pp. 1-6, 2019.

22.V. Le, T. P. Quinn, T. Tran and S. Venkatesh, "Deep in the bowel: Highly interpretable neural encoder-decoder networks predict gut metabolites from

gut microbiome", *BMC Genomic.*, vol. 21, no. 4, pp. 1-15, 2020.

23.S. Golovkine, N. Klutchnikoff and V. Patilea, "Clustering multivariate functional data using unsupervised binary trees", *Comput. Statist. Data Anal.*, vol. 168, 2022, [online] Available: https://www.sciencedirect.com/science/article/pii/S0167947321002103.

24.K. P. Sinaga and M.-S. Yang, "Unsupervised k-means clustering algorithm", *IEEE Access*, vol. 8, pp. 80716-80727, 2020.

25.R. Taormina et al., "Battle of the attack detection algorithms: Disclosing cyber attacks on water distribution networks", *J. Water Resour. Plan. Manage.*, vol. 144, no. 8, 2018.