International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

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

CH NIKHIL[1], PSVK LALITH VISWAS[2], J SAI PRANEETH[3], T MAHEETH[4], G.VARAHA GIRI[5]

[1,2,3,4] UG students, Dept of CSE(CS), Malla Reddy Engineering College (Autonomous), Secunderabad, Telangana State

[5]Assistant Professor, Dept of CSE(CS), Malla Reddy Engineering College (Autonomous), Secunderabad, Telangana State

ABSTRACT

In order to improve data safety and security, several sectors are now developing blockchain-based contemporary solutions. A blockchain-based network is among the most notable uses of blockchain technology within the framework of the IIoT. Industrial Internet of Things (IIoT) devices are becoming more common in our digital environment, particularly for the purpose of building smart factories. Despite its usefulness, blockchain technology is vulnerable to cyber attacks. In order to protect networks and systems from unforeseen attacks, it is necessary to detect abnormalities in smart manufacturing facilities' blockchain-based IIoT networks. In this article, we build a threat hunting framework named Block Hunter using Federated Understanding (FL) to instantly search for attacks on IIoT networks that are built on blockchain. In a federated setting, Block Hunter employs a cluster-based approach for anomaly identification that incorporates many machine learning versions. Our research indicates that Block Seeker is the first federated risk hunting version for IIoT networks to identify suspicious patterns while protecting user privacy. Our results show that the Block Seeker is effective in detecting suspicious activity with a high degree of precision and a low amount of transmission capacity required.

Keywords: FL, Block hunter, IIOT, High security data, IOT.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

I INTRODUCTION

Blockchain technology is becoming a useful tool in many fields, including healthcare, the military, finance, and networking, thanks to its immutable and tamper-proof data security features. Factories, in particular, are becoming more intelligent and efficient as a result of technological advancements, and this trend is driven by the ever-increasing use of Industrial Internet of Things (IIOT) solutions. [1] One subset of the Internet of Things (IoT) is the Industrial Internet of Things (IIOT). Nevertheless, when it comes to the requirements for safety and security, IIOT and IOT are diverse. While the IIOT improves the quality of life for consumers, its primary goal is to strengthen production security, efficiency, and safety. When it comes to business-to-business (B2B) environments, IIOT tools are more often employed, but IOT devices are more commonly considered in business-to-customer (B2C) settings. Because of this, the risk profile for IIOT networks would be different from that of their IOT equivalents, where device-to-device transactions are very valuable.

IIoT networks allow us to meet the demands of our clients and support a wide range of applications, especially in industrial settings like smart factories. [1] Smart factories, smart homes/buildings, smart farms, smart cities, connected drones, and medical care systems are just a few examples of the IIOT-based networks that have embraced blockchain technology due to its many benefits [1, 2]. This research primarily focuses on smart manufacturing facility block chain-based IIoT network security [3, 4], however the suggested architecture might be applied to other IIoT environments as well.

Modern smart factories use Internet-enabled lighting, temperature monitoring systems, IP electronic cameras, and IP phones to power a plethora of operations that rely on these technologies. These devices are storing confidential information and could provide answers that are vital to public safety. in [3], (1) The primary issue will undoubtedly be the secure storage,

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

accumulation, and exchange of data as the number of IIOT devices in smart factories increases. Consequently, in this kind of situation, industrial, critical, and personal data are all at risk. With blockchain technology, data integrity, strong authentication, and a reliable timetable for communication foundations can be guaranteed both inside and outside of smart manufacturing plants. However, there are still significant obstacles to privacy and security in IIOT [3, 4]. An key challenge with blockchain-based networks is the potential of misleading tasks occurring in them [2, 4]. Blockchain technology is a powerful tool, but it is not immune to cyberattacks. Case in point: Ethereum Standard was hit by a 51% cyber attack [2] and three consecutive strikes in August 2020 [5], leading to the loss of more than $5 million worth of cryptocurrency. These incidents have shown the vulnerabilities of this blockchain network.

During transmission, utilisation, and storage, smart factories must protect the privacy of consumers' information. [4] Scammers may access, alter, or utilise the stored data for malicious purposes, making it susceptible to interference. When looking at the data, these assaults stand out as unusual occurrences that don't follow the norm. [2, 6] For threat hunting programmes and for safeguarding systems against unauthorised access, the ability to detect and filter out-of-the-ordinary activities is essential. the references [6], [7]

The primary objective of this article is to identify dubious clients and transactions inside an IIOT network that is built on blockchain technology, with a focus on smart manufacturing facilities. In this case, out-of-character actions stand in for dubious routines. [4] Machine learning (ML) techniques may be used to detect strikes and abnormalities on the blockchain by finding trends and outliers. Deep neural networks are a promising alternative for anomaly detection since they autonomously learn representations from training data. [4, 7] However, problems might arise with anomaly finding systems that rely on machine learning or deep learning. Concerns about privacy and a lack of

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

training data are addressed by these methods. [7]

It is difficult to detect anomalies on the blockchain. [8] Not only does sending each block to a main server increase training time, but the version also needs fresh block data during testing [8]. Furthermore, malevolent adversaries might use causal/data poisoning attacks to intentionally damage the ML architecture when ML models are routinely updated to respond to new dangers and identify anomalies. To avoid detection of anomalies, attackers may deliberately send out designed payloads.

Using Federated Discovering (FL) architectures to detect anomalies while safeguarding personal information and monitoring data quality is a novel and practical technique. references [7], [9] With FL, edge devices may work together during training while keeping all data locally. Instead of transmitting the data to another place, we may train the model locally on the device, and then communicate just the most recent modifications with the rest of the network.

One recent trend in machine learning is FL, which allows for smart edge devices to make mutual predictions with one another [7], [10]. Also, FL handles crucial issues with data sharing, information security, and digital civil liberties management, and it ensures that several stars build long-lasting machine finding designs without exchanging data. This research adopts an anomaly-detection structure called Block Seeker that is based on FL and can identify attack hauls in IIOT networks that are built on the blockchain, according to these features.

This study primarily contributes to the following areas:

First, create an anomaly detection problem for smart factories that use blockchain technology by using a cluster-based architecture. When it comes to reducing transmission capacity and increasing throughput in IIoT networks, the cluster-based approach improves hunting effectiveness.

2) Identify suspicious activity in IIoT devices linked to smart factories that use blockchain technology by implementing a federated design version. In a

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

federated setting, this provides a privacy-preserving function for machine learning versions.

3.) Applying several methods for finding abnormalities, such as clustering-based, analytical, subspace-based, classifier-based, and tree-based, to efficiently identify abnormalities in smart factories.

4) The Block Hunter structure is examined in relation to block production, block size, and miners. True Positive Rate (TPR) anomaly detection, F1-score, Precision, and Recall are some of the performance metrics that are examined.

SURVEY OF RESEARCH

Digital bitcoin transactions may be analysed with the use of an algorithm that was suggested by Sayadi et al. [5]. In order to classify outliers that were similar in kind and statistical importance, they looked at the K-means and One-Class Support Vector Machines (OCSVM) algorithms. After reviewing their work via the creation of discovery results, they discovered that we can get excellent results in terms of accuracy.

Anomaly semantics in blockchain-based IoT networks was the basis for the authors' proposed solution in [6]. An approach was already in place to detect suspicious activity in blockchains by gathering metadata in forks and using it to determine common informational identification of unusual tasks. They developed a device that improves the security of blockchains and interconnected devices. Similarly, in order to discover blockchain security, has really presented encoder-decoder deep learning regression in [7]. An anomaly finding framework based on collected data from bitcoin blockchain monitoring was constructed in this study. Their testing has shown that their system can detect publicly known attacks by mining the Ethereum network's previous records.

The authors Chai et al. [2] suggested using FL and a hierarchical blockchain structure to discover and exchange environmental data. For large-scale vehicle networks, this design is practical and dependable. The distributed pattern and personal privacy demands of the Net of Autos are met by FL-based discovery. Knowledge sharing is encouraged via the use of a model that

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

mimics a multi-leader, multi-player trading market mechanism. The results of the substitution show that an ordered structure-based approach may improve the sharing, discovery, and handling of specific harmful attacks. Furthermore, the authors of [3] provide an exhaustive analysis of how FL might offer enhanced cybersecurity and evade many attackers simultaneously. This study identifies key challenges and opportunities for further research on FL's implementation in real-world settings.

PROPOSED SYSTEM

Automatically protecting a system from unforeseen attacks relies heavily on detecting suspicious behaviours. In order to detect blockchain anomalies, every time a block is upgraded, the data from that block must be sent to a central server. In addition to being ineffective, this raises issues of individual privacy. When it comes to addressing this issue, FL options appear promising. To discover anomalies, we utilise FL to get an international version of the model and to update it periodically. Once we have gathered information on each smart factory's data, devices, and business, we will send the version's specs to the parameter server so that we can aggregate them and improve our core design. With collection-based architecture, the blockchain can function in any smart factory with much more dependable usage sources and throughput. Clustering simplifies the hierarchical hidden network construction process in terms of computational complexity.

WORKING METHODOLOGY

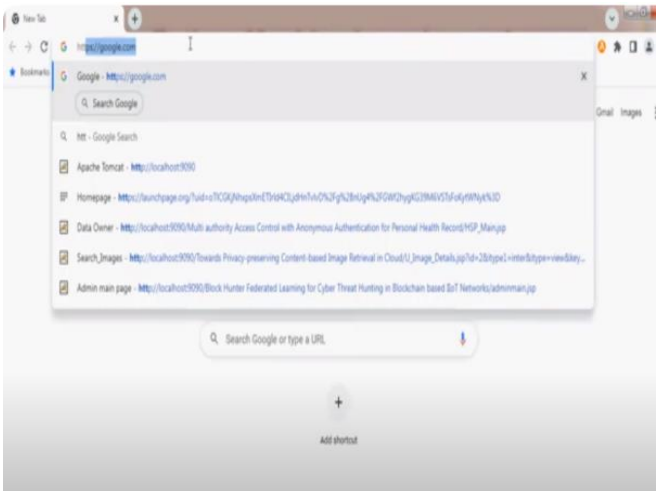

Fig.1. Home page.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

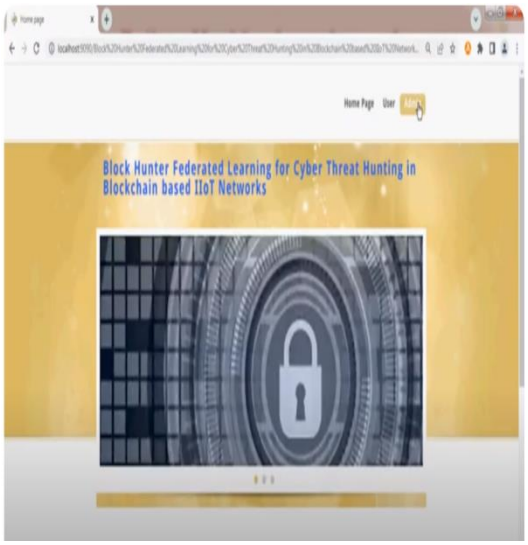

Fig.2. Home page.

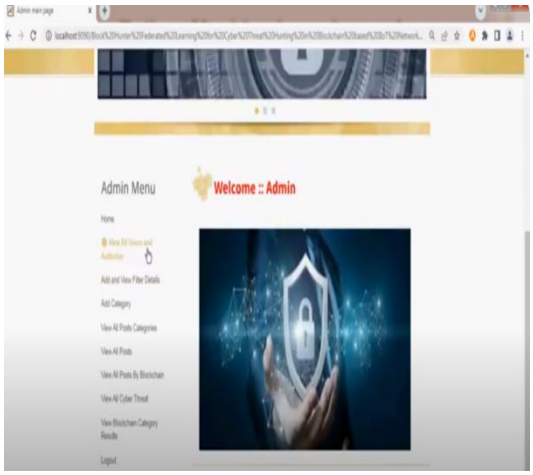

Fig.3. Admin login page.

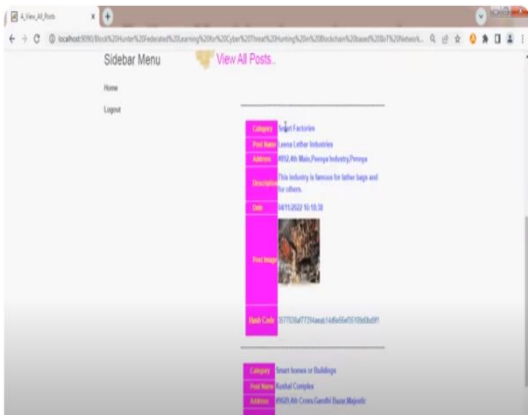

Fig.4. All details of users.

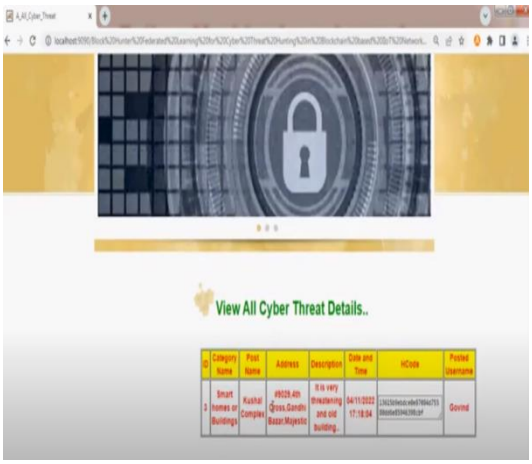

Fig.5. Cyber thefts details.

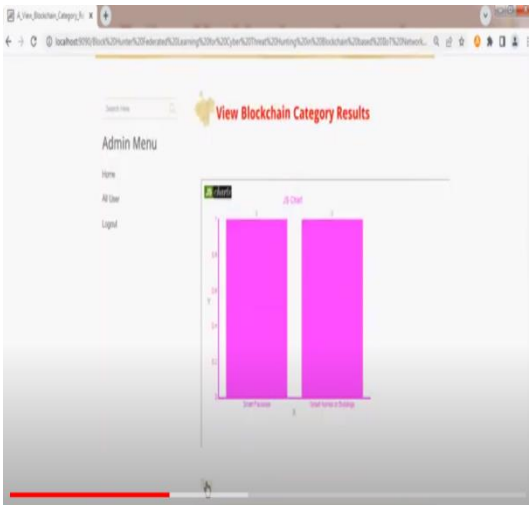

Fig.6. Output results.

In the intelligent sectors, IIoT tools are often used. Although blockchain is secure, it may be hacked. In order to protect themselves against assaults, smart manufacturing facilities that use blockchain-based IIoT networks need to detect issues. Block seeker is a threat-hunting framework that hunts for dangers in blockchain-based IIoT

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

networks automatically. It is constructed using federated learning. When looking for anomalies, block hunter employs federated maker learning designs with a cluster-based architecture. A privacy-preserving, federated danger-hunting method called "block hunter" for IIoT networks. When using the FedAvg approach with a discovery rate of 95%, the block hunter is able to accurately identify suspicious behaviours even when bandwidth is limited.

CONCLUSION

Using a federated understanding approach, we built the Block Hunter framework in this article to seek for anomalies in IIOT smart factories that are based on the blockchain. To improve the search performance of IIOT networks that utilise blockchain technology and reduce their associated sources, Block Hunter employs a cluster-based design. We used several AI techniques (NED, IF, CBLOF, K-means, PCA) to look for anomalies in the Block Seeker framework. The effects of block size, block creation interval, and the number of miners on Block Seeker performance were also investigated. An intriguing area for future research may be the use of generative adversarial networks (GAN) to build and run a framework similar to block hunters. It would also be worthwhile to investigate, down the road, the possibility of developing and implementing IIOT-related blockchain connections with other agreement formulae.

ACKNOWLEDGMENT

We thank CMR Technical Campus for supporting this paper titled "**BLOCK HUNTER FEDERATED LEARNING FOR CYBER THREAT HUNTING IN BLOCKCHAIN-BASED IIOT NETWORKS**", which provided good facilities and support to accomplish our work. I sincerely thank our Chairman, Director, Deans, Head of the Department, Department Of Computer Science and Engineering, Guide and Teaching and Non- Teaching faculty members for giving valuable suggestions and guidance in every aspect of our work.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

REFERANCES

[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 Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3652–3660, 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 (ICAR), 2019, 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. Elsevier, 2020, pp. 157–181.

[4] B. Podgorelec, M. Turkanovi´c, and S. Karakati˘c, "A machine learningbased method for automated blockchain transaction signing including personalized anomaly detection," Sensors, vol. 20, no. 1, p. 147, 2020.

[5] A. Quintal, "Veriblock foundation discloses mess vulnerability in ethereum classic blockchain," VeriBlock Foundation. [Online]. Available: https://www.prnewswire. com/news-releases/veriblock-foundation-discloses-mess-vulnern ability-in-ethereum-classic-blockchain-301327998.html

[6] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1977–2008, 2020.

[7] R. A. Sater and A. B. Hamza, "A federated learning approach to anomaly detection in smart buildings," arXiv preprint arXiv:2010.10293, 2020.

[8] O. Shafiq, "Anomaly detection in blockchain," Master's thesis, Tampere University, 2019.

[9] A. Yazdinejadna, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "Federated learning for drone authentication," Ad Hoc Networks, p. 102574, 2021.

[10] 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," Applied Sciences, vol. 8, no. 12, p. 2663, 2018.

[11] L. Tan, H. Xiao, K. Yu, M. Aloqaily, and Y. Jararweh, "A blockchainempowered crowdsourcing system for 5g-enabled smart cities," Computer Standards & Interfaces, vol. 76, p. 103517, 2021.

[12] L. Tseng, X. Yao, S. Otoum, M. Aloqaily, and Y. Jararweh, "Blockchainbased database in an iot environment: challenges, opportunities, and analysis," Cluster Computing, vol. 23, no. 3, pp. 2151–2165, 2020.

[13] M. Signorini, M. Pontecorvi, W. Kanoun, and R. Di Pietro, "Bad: a blockchain anomaly detection solution," IEEE Access, vol. 8, pp. 173 481–173 490, 2020.

[14] S. Iyer, S. Thakur, M. Dixit, R. Katkam, A. Agrawal, and F. Kazi, "Blockchain and anomaly detection based monitoring system for enforcing wastewater reuse," in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2019, pp. 1–7.

[15] S. Sayadi, S. B. Rejeb, and Z. Choukair, "Anomaly detection model over blockchain electronic transactions," in 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). IEEE, 2019, pp. 895–900.