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

CYBER THREAT HUNTING IN BLOCKCHAIN-ENABLED IIOT NETWORKS USING BLOCKHUNTER AND FEDERATED LEARNING

[1]VARUN MARAMRAJ, [2]MADDI APARNA
[1]Assistant Professor,[2]Student
Department of CSE
Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT

Blockchain-based solutions are now being developed to enhance data security across several sectors. One of the most prominent uses of blockchain technology in the context of the Industrial Internet of Things (IIoT) is a chain-based network. In our digital age, IIoT devices are becoming more and more common, particularly as they aid in the development of smart factories. Despite its strength, blockchain remains susceptible to cyberattacks. In order to safeguard networks and systems against unforeseen assaults, it is essential to identify abnormalities in blockchain-based IIoT networks in smart factories. In this research, we develop a threat hunting system, named Block Hunter, to automatically search for threats in blockchain-based IIoT networks using Federated Learning (FL). Block Hunter employs many machine learning models in a federated environment together with a cluster-based architecture for anomaly detection. As far as we are aware, Block Hunter is the first federated threat hunting approach that protects privacy in IIoT networks by detecting unusual activity. Our findings demonstrate the effectiveness of the Block Hunter in accurately and efficiently identifying unusual activity with the least amount of bandwidth needed.

1. INTRODUCTION

Blockchain's immutable and tamperproof data security features make it a viable tool in many fields, including healthcare, banking, and networking, thanks to its technical trajectory. The world is unavoidably becoming a smarter, more connected place with the growing usage of Industrial Internet of Things (IIOT) devices; as technology develops, factories in particular are getting more intelligent and productive [1]. The Internet of Things is thought to include IIOT as a subclass (IOT). However, in terms of security needs, IIOT and IOT vary from one another. The goal of the IIOT is to improve manufacturing efficiency and safety while also making customers' life simpler and more pleasant. IOT devices are mostly taken into consideration in B2C (business-to-consumer) contexts, while IIOT devices are primarily employed in B2B (business-to-business) settings. As a result, IIOT networks would have a distinct threat profile than their IOT equivalents, where device-to-device interactions are crucial.

IIOT networks provide us a broad platform to enable a multitude of

Index in Cosmos
Oct 2024, Volume 14, ISSUE 4
UGC Approved Journal

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

applications and equip us to address user demands, particularly in an industrial context like smart factories [1]. The benefits of blockchain technology have made it widely used in IIOT-based networks, including linked drones, healthcare systems, smart buildings, smart factories, smart farms, and smart cities [1], [2]. Although the security of blockchain-based IIOT networks in smart factories is the main emphasis of this article [3], [4], other IIOT contexts may also make use of the proposed architecture.

Modern smart factories include a large number of linked equipment, including IP cameras, IP phones, Internet-enabled lighting, and temperature monitoring systems, supporting a wide range of operations. These gadgets may provide services that are vital to safety while also preserving private and sensitive data. [3], [1]. The primary challenge will be securely storing, gathering, and exchanging data as the number of IIOT devices in smart factories rises. Therefore, in such a scenario, industrial, critical, and personal data are at danger. By using robust authentication and guaranteeing the availability of communication backbones, block chain technology can guarantee data integrity both within and outside of smart factories. In spite of this, privacy and security concerns pose serious obstacles for IIOT [3], [4]. An additional concern is the likelihood of fraudulent conduct in block chain-based networks [2, 4]. Although block chain technology is an effective instrument, cyberattacks may still occur. Examples of the weaknesses of this block chain network include a 51% cyber assault [2] on Ethereum Classic and three separate attacks in August 2020 [5], which led to the loss of almost $5 million in cryptocurrency.

Users' privacy should be safeguarded in smart factories throughout data transmission, use, and storage. [4]. Data that has been stored makes it susceptible to manipulation by scammers who want to access, change, or utilise it for nefarious purposes. From a statistical perspective, these assaults might be considered abnormal occurrences because they significantly deviate from typical behaviour [2], [6]. Threat hunting programs depend on the automated detection and filtering of unusual actions, which helps safeguard systems against unauthorised access. [6], [7].

This article aims to identify suspicious transactions and users in a block chain-based IIOT network designed for smart factories. Here, aberrant behaviour also functions as a stand-in for questionable behaviour [4]. We may use Machine Learning (ML) methods to detect attacks and anomalies on block chains by using outlier and pattern identification to recognise patterns that deviate from the norm. Deep neural networks are a potential option for anomaly detection since they automatically learn representations from the data they are trained on [4], [7]. All machine learning and deep learning-based anomaly detection methods, nevertheless, have drawbacks. These techniques include privacy concerns as well as challenges with the shortage of training data [7].

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

Finding irregularities in the block chain is a challenging problem [8]. The model needs fresh block data for testing, in addition to the fact that every block must be uploaded to a central server, which lengthens the training period [8]. In addition, hostile attackers may use causation or data poisoning attacks to purposefully weaken the ML model while it is regularly updated to address new threats and identify irregularities. To avoid anomaly detection, attackers could purposefully deliver carefully constructed payloads.

Federated learning (FL) models are an innovative and useful method to monitor data quality and discover abnormalities while maintaining data privacy [7], [9]. During the training phase, FL enables edge devices to work together while all data remains on the device. Rather of transferring the data to a different location, we may train the model locally on the device, and just the model's changes are sent across the network.

The ability of smart edge devices to concurrently generate mutual predictions with one another has made FL a popular approach in machine learning [7], [10]. Furthermore, FL addresses key privacy, data security, and digital rights management concerns by ensuring various parties build strong machine learning models without sharing data. In light of these features, this study employs Block Hunter, a FL-based anomaly-detection framework, to identify attack payloads in block chain-based IIOT networks.

The following is a summary of the paper's primary contributions:

1) Create an anomaly detection issue in block chain-based smart factories using a cluster-based architecture. In IIoT networks, the cluster-based strategy improves hunting efficiency in terms of throughput and bandwidth reduction.

2) Use a federated design paradigm to identify unusual activity in IIoT devices connected to smart factories built on blockchain. This offers a function that protects privacy when using federated frameworks with machine learning models.

3) The use of many anomaly detection techniques, including statistical, subspace, classifier, clustering, and tree-based approaches, can effectively identify anomalies in smart factories.

4) The effects on the Block Hunter framework of miners, block size, and block production are taken into account. Furthermore included are performance metrics such as True Positive Rate (TPR) anomaly detection, Accuracy, Precision, Recall, and F1-score.

The remainder of the paper is broken down here. The work on anomaly detection in FL and the block chain is covered in Section II. The Block Hunter framework, network concept, and topology design are presented in Section III. Methodologies and machine learning techniques for detecting abnormalities are covered in Section IV. We provide the evaluation of the Block Hunter framework in Section V. Lastly, We wrap up the study

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

and outline future prospects for research in Section VI.

2. LITERATURE SURVEY

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.

In the contemporary digital age, the assurance of privacy and security in online transactions remains a paramount concern. This research meticulously introduces and investigates a ground-breaking blockchain-based framework, specifically tailored to address and enhance these aspects. The principal objective of this study is to offer a comprehensive solution to a spectrum of challenges currently prevalent in existing transaction systems. Traditional systems often grapple with a host of issues, including vulnerability to security breaches, inadequate privacy safeguards, latency in transaction processing, and challenges in scalability. These systems, often centralized, present single points of failure and frequently fall short in offering robust privacy-preserving mechanisms. To mitigate these challenges and bridge the gaps identified in the current landscape, the proposed framework ingeniously amalgamates advanced cryptographic techniques, decentralized protocols, and smart contracts. The design ensures a robust and transparent mechanism that eliminates single points of failure, thereby significantly enhancing security. The methodology adopted in this research involves a thorough evaluation and assessment of the proposed framework against a series of key metrics. These include security robustness, privacy assurance, transaction throughput, latency, and cost-effectiveness, among others. The findings from this study underscore several noteworthy achievements of the proposed framework. It exhibits a remarkable increase in transaction throughput, processing at a rate that is approximately double compared to existing systems. Additionally, the latency observed in the transaction confirmation process is significantly reduced, ensuring swift and efficient transactions. The framework also demonstrates a robust resistance to common security threats and attacks. Furthermore, the implementation ensures user anonymity and privacy are upheld through cryptographic techniques, thereby addressing privacy concerns prevalent in current systems. Optimal resource utilization is maintained, ensuring the framework is not only secure and private but also efficient. In conclusion, this research presents a compelling case for the adoption of the proposed blockchain-based framework as a potent solution to the myriad of issues identified in existing transaction systems. The study contributes significantly to the discourse on secure and privacy-preserving online transactions, presenting a framework that is not only theoretically sound but also practically viable.

F. Scicchitano, A. Liguori, M. Guarascio, E. Ritacco, and G. Manco, "Blockchain

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

attack discovery via anomaly detection," ConsiglioNazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni(ICAR), 2019, 2019.

In these last years, Blockchain technologies have been widely used in several application fields to improve data privacy and trustworthiness and security of systems. Although the blockchain is a powerful tool, it is not immune to cyber attacks: for instance, recently (January 2019) a successful 51% attack on Ethereum Classic has revealed security vulnerabilities of its platform. Under a statistical perspective, attacks can be seen as an anomalous observation, with a strong deviation from the regular behavior. Machine Learning is a science whose goal is to learn insights, patterns and outliers within large data repositories; hence, it can be exploit for blockchain attack detection. In this work, we define an anomaly detection system based on a encoder-decoder deep learning model, that is trained exploiting aggregate information extracted by monitoring blockchain activities. Experiments on complete historical logs of Ethereum Classic network prove the capability of the our model to e↵ectively detect the publicly reported attacks. To the best of our knowledge, our approach is the first one that provides a comprehensive and feasible solution to monitor the security of blockchain transactions.

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.

Security, privacy, and transparency aspects of the Internet of Things (IoT) sensors have recently raised significant concerns among the public and policymakers. The distributed ledger and Blockchain technologies had brought solutions through transparently bridging two or multiple untrusted parties. In this research, a novel architecture for a smart building system, including a control system and automatic approaches, is proposed. An efficient cluster head selection algorithm is proposed to select the desired cluster head with the consideration of low energy consumption and fast head selection. An enhanced combination of IoT forwarding devices and Software-Defined Networking (SDN) technology is further advanced. Furthermore, the proposed "DistBlockBuilding" architecture is implemented for managing a safe and secure data transfer from one surface to another surface. Besides, Blockchain technology is performed for transferring data within the smart building. Finally, the performance of IoT-SDN based secured networks is evaluated.

3. EXISTING SYSTEM

The research by Sayadi et al. [15] proposes an algorithm for anomaly detection over bitcoin electronic transactions. They examined the One-Class Support Vector Machines (OCSVM) and the K-means algorithms to group outliers similar in both

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

statistical significance and type. They analyzed their work by generating detection results and found that we could obtain high-performing results on accuracy.

In [16], the authors suggested an approach based on the semantics of anomalies in blockchain-based IoT Networks. A method was presented to detect anomalous behavior in blockchain that gathers metadata in forks to determine mutual informational recognition of anomalous activity. They developed a tool that improves blockchain security and connected devices. Also, in [17], has introduced encoder-decoder deep learning regression for detecting blockchain security. This work developed an anomaly detection framework that relies on aggregate information derived from bitcoin blockchain monitoring. Their experiments have demonstrated that their model can detect publicly reported attacks using the historical logs of the Ethereum network.

Chai et al. [22] proposed a hierarchical blockchain framework and FL to learn and share environmental data. This framework is functional and efficient for large-scale vehicular networks. FL-based learning meets the Internet of Vehicles' distributed pattern and privacy requirements. Sharing behavior is modeled as a multi-leader, multi-player trading market process to stimulate knowledge sharing. Simulated results indicate that an algorithm based on hierarchical structures can enhance sharing, learning, and managing specific malicious attacks. Furthermore, the authors in [23] deliver a comprehensive investigation on how FL could supply better cybersecurity and prevent various cyberattacks in real-time. This work highlights some main challenges and future directions on which the researchers can focus for adopting FL in real-time scenarios.

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.

4. PROPOSED SYSTEM

Detecting anomalous activities is a significant contributor to automatically protecting a system from unexpected attacks. Anomalies in blockchain must be detected by sending each block of data to a central server for each block update. This is not efficient and also imposes privacy concerns. FL solutions are promising in tackling this issue. We use FL to update the model frequently and to obtain a global model for detecting an anomaly. After learning about each smart factory's data, devices, and service provider, the model's parameters will be sent to the parameter server for aggregation and to update our general model.

Cluster based architecture provides more efficient use of resources and throughput during the blockchain run in each smart

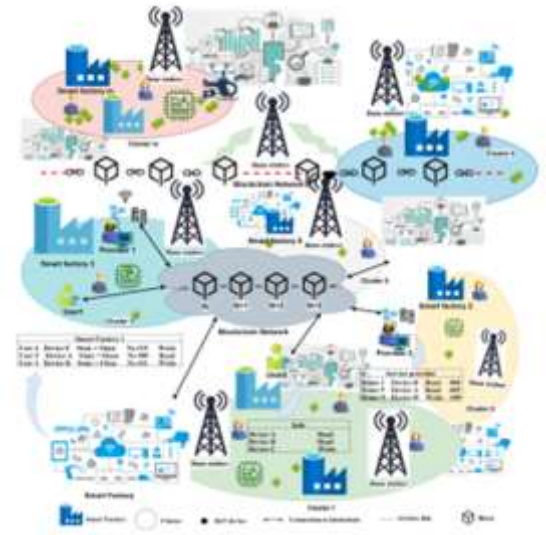
International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

factory. Clustering reduces the computational complexity in the creation of the underlying network through a hierarchical approach.

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.

5. SYSTEM ARCHITECTURE



6. IMPLEMENTATION

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, Train & Test IIOT Network Datasets, View Trained and Tested IIOT Network Datasets Accuracy in Bar Chart, View Trained and Tested IIOT Network Datasets Accuracy in Bar Chart, 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.

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 CYBER THREAT HUNTING TYPE, VIEW YOUR PROFILE.

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

7. CONCLUSION AND FUTURE ENHANCEMENT

In this research, we created a federated learning strategy to hunt anomalies in block chain-based IIOT smart factories: the Block Hunter framework. Block Chain-based IIOT network searching can be done more efficiently and with lower resource consumption thanks to Block Hunter's cluster-based design. A range of machine learning methods (NED, IF, CBLOF, K-means, PCA) were used to assess the Block Hunter framework in order to find abnormalities. We also looked at how various miners, block sizes, and block creation intervals affected the Block Hunter's performance. It would be interesting to do more study on designing and implementing a block hunter-like framework using generative adversarial networks (GAN). Additionally, it would be worthwhile to look at developing and implementing IIOT-related block chain networks using various consensus algorithms in the future.

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 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,

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

"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 block chain empowered 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.

[16] Z. Il-Agure, B. Attallah, and Y.-K. Chang, "The semantics of anomalies in iot integrated blockchain network," in 2019 Sixth HCT Information Technology Trends (ITT). IEEE, 2019, pp. 144–146.

[17] F. Scicchitano, A. Liguori, M. Guarascio, E. Ritacco, and G. Manco, "A deep learning approach for detecting security attacks on blockchain." In ITASEC, 2020, pp. 212–222.

[18] T. R. Gadekallu, Q.-V. Pham, D. C. Nguyen, P. K. R. Maddikunta, N. Deepa, B. Prabadevi, P. N. Pathirana, J. Zhao, and W.-J. Hwang, "Blockchain for edge of things: Applications, opportunities, and challenges," IEEE Internet of Things Journal, vol. 9, no. 2, pp. 964–988, 2022.

[19] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, "D¨ıot: A federated self-learning anomaly detection system for iot," in 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2019, pp. 756–767.

[20] S. Li, Y. Cheng, Y. Liu, W. Wang, and T. Chen, "Abnormal client behavior detection in federated learning," arXiv preprint arXiv:1910.09933, 2019.