IJITCE

ISSN 2347- 3657

International Journal of
Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

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

[1] A NAGARAJU, [2]P.CHARAN TEJA

[1](Assistant Professor), MCA, **DANTULURI NARAYANA RAJU COLLEGE(A) PG COURSES, BHIMAVARAM ANDHRA PRADESH**

[2]MCA, scholar, **DANTULURI NARAYANA RAJU COLLEGE(A) PG COURSES, BHIMAVARAM ANDHRA PRADESH**

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 cyber attacks. Detecting anomalies in blockchain-based IIoT networks in smart factories is crucial in protecting networks. and systems from unexpected attacks. In this paper, we use Federated Learning (FL) 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.

1.INTRODUCTION

THE technological trajectory of block chain makes it a valuable tool in many areas, including healthcare, military, finance and networking, via its immutable and tamperproof data security advantages. With the ever-increasing use of Industrial Internet of Things (IIOT) devices, the world is inevitably becoming a smarter interconnected environment; especially factories are becoming more intelligent and efficient as technology advances [1]. IIOT is considered a subcategory of the Internet of Things (IOT). There are, however, differences between IOT and IIOT in terms of security requirements. While the IIOT makes consumers' lives easier and more convenient, the IIOT aims to increase production safety and efficiency. IIOT devices are mainly used in B2B (business-to-business) settings, while IOT devices are mostly considered in B2C (business-to consumer) environments. This would lead to a different threat profile for IIOT networks compared to their IOT counterparts where device-to-device transactions are of utmost importance.

IIOT networks provide an umbrella for supporting many applications and arm us to respond to users' needs, especially in an industry setting such as smart factories [1]. Block chain technology advantages lead to its wide adoption in IIOT based networks such as smart factories, smart homes/buildings, smart farms, smart cities, connected drones, and healthcare systems [1], [2]. While the focus of this paper is on the security of block chain-based IIOT networks in smart factories [3], [4], the suggested framework may be used in other IIOT settings as well.

In modern smart factories, many devices are connected to the public networks, and many activities are supported by smart systems such as temperature monitoring systems, Internet-enabled lights, IP cameras, and IP phones. These devices are storing private and sensitive data and may offer safety-critical services [3], [1]. As the number of IIOT devices in smart factories increases, the main issue will be storing, collecting, and sharing data securely. Industrial, critical, and personal data are therefore at risk in such a situation. Block chain technology can ensure data integrity inside and outside of smart factories through strong authentication and ensure the availability of communication backbones. Despite this, privacy and security issues are significant challenges in IIOT [3], [4]. The probability of fraudulent activity occurring in block chain-based networks [2], [4] is an important issue. Even though block chain technology is a powerful tool, it is not protected from cyber attacks

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

either. For example, a 51% cyber attack [2] on Ethereum Classic, and three consecutive attacks in August of 2020 [5], which resulted in the theft of over $5M worth of crypto currency, have exposed the vulnerabilities of this block chain network.

Smart factories should protect users' data privacy during transmission, usage, and storage [4]. Stored data are vulnerable to tampering by fraudsters seeking to access, alter or use the data with malicious motives. Statistically speaking, these attacks can be viewed as anomalous events, exhibiting a strong

deviation from usual behavior [2], [6]. Detecting out-of-norm events are essential for threat hunting programs and protecting systems from unauthorized access by automatically identifying and filtering anomalous activities. [6], [7].

The main objective of this paper is to detect suspicious users and transactions in a block chain-based IIOT network specifically for smart factories. Here, abnormal behavior serves as a proxy for suspicious behavior as well [4]. By identifying outliers and patterns, we can leverage Machine Learning (ML) algorithms to identify out-of-norm patterns to detect attacks and anomalies on block chain. Because deep neural networks learn representations automatically from data that they are trained on, they are the candidate solution for detecting

anomalies [4], [7]. However, there are challenges with any ML and deep learning-based anomaly detection techniques. These methods suffer from training data scarcity problems, and privacy issues [7].

Detecting anomalies in the block chain is a complicated issue [8]. Not only each block needs to be sent to a central server, which increases the training time, but also the model requires new block data in the testing phase [8]. In addition, when ML models are frequently updated to respond to new threats and detect anomalies, malicious adversaries can launch causative/data poisoning attacks to degrade the ML model deliberately. Attackers may intentionally send crafted payloads to evade anomaly detection.

A novel and practical approach would be to employ Federated learning (FL) models to detect anomalies while preserving data privacy, and monitoring data quality [7], [9]. FL allows edge devices to collaborate during the training stage while all data stays on the device. We can train the model on the device itself instead of sending the data to another place, and only the updates of the model are shared across the network.

FL has become a trend in ML where smart edge devices can simultaneously develop a mutual prediction between each other [7], [10]. In addition, FL ensures multiple actors construct robust machine learning models without sharing data, addressing fundamental privacy, data security, and digital rights management challenges. Considering these characteristics, this paper uses an FL-based anomaly-detection framework called Block Hunter capable of detecting attack payloads in block chain-based IIOT networks

The main contributions of the paper are summarized as follows:

1) Utilize a cluster-based architecture to formulate an anomaly detection problem in block chain-based smart factories. The cluster-based approach increase hunting efficiency in terms of bandwidth reduction and throughput in IIoT networks.

2) Apply a federated design model to detect anomalous behaviour in IIoT devices related to blockchain-based smart factories. This provides a privacy-preserving feature when using machine learning models in a federated framework.

3) Implementation of various anomaly detection algorithms such as clustering-based, statistical, subspace-based, classifier-based, and tree-based for efficient anomaly detection in smart factories.

4) The impact of block generation, block size, and miners on the Block Hunter framework are considered. Moreover, the performance measurements like Accuracy, Precision, Recall, F1-score, and True Positive Rate (TPR) anomaly detection are discussed.

Here is a breakdown of the rest of the paper. Section II discusses anomaly detection works in the block chain and FL. Section III describes the Block Hunter framework and presents the network model and topology design. In Section

IV, methodology and machine learning approaches to identify anomalies are discussed. In Section V, we present the assessment of the Block Hunter framework. Finally, In Section VI, we conclude the paper and point out future work directions.

2. 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 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.

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

- ❖ The system is not implemented Cluster-Based Local Outlier Factor.

3. 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 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.

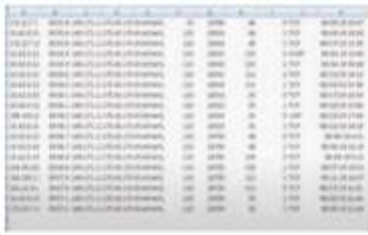
Model Aggregation (FedAvg): Parameter server aggregates model weights to compute an enhanced global model.

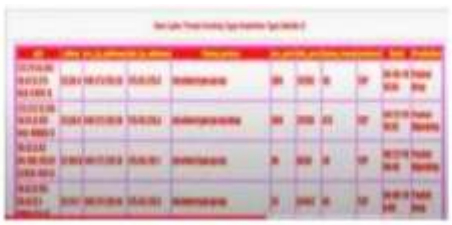
4.OUTPUTSCREENS

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024





5.CONCLUSION

In this paper, we developed the Block Hunter framework to hunt anomalies in block chain-based IIOT smart factories using a federated learning approach. Block Hunter uses a cluster-based architecture to reduce resources and improve the throughput of block chain-based IIOT networks hunting. The Block Hunter framework was evaluated using a variety of machine learning algorithms (NED, IF, CBLOF, K-means, PCA) to detect anomalies. We also examined the impacts of block generation interval, block size, and different miners on the performance of the Block Hunter. Using generative adversarial networks (GAN) to design and implement a block hunter like framework would be an interesting future research work. Furthermore, designing and applying IIOT-related block chain networks with different consensus algorithms would also be worth investigating in the future.

7. REFERENCES

[1] J. Wan, J. Li, M. Imran, D. Li, and F. e Amin, “A blockchain-basedsolution for enhancing security and privacy in smart factory,” IEEETransactions 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," ConsiglioNazionale 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 effectiveblockchain-based, decentralized application for smart building systemmanagement," in Real-Time Data Analytics for Large Scale Sensor Data.Elsevier, 2020, pp. 157–181.

[4] B. Podgorelec, M. Turkanovi´c, and S. Karakatiˇc, "A machine learningbasedmethod for automated blockchain transaction signing includingpersonalized anomaly detection," Sensors, vol. 20, no. 1, p. 147, 2020.

[5] A. Quintal, "Veriblock foundation discloses messvulnerability in ethereum classic blockchain," VeriBlockFoundation. [Online]. Available: https://www.prnewswire.com/news-releases/veriblock-foundation-discloses-mess-vulnernability-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: Acomprehensive 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 anomalydetection in smart buildings," arXiv preprint arXiv:2010.10293, 2020.

[8] O. Shafiq, "Anomaly detection in blockchain," Master's thesis, TampereUniversity, 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 federatedlearning: An intrusion detection case study," Applied Sciences, vol. 8,no. 12, p. 2663, 2018.