INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

CYBER THREAD PREDICTION IN SMART FACTORIES

[1] Dr. A. Satyanarayana, Professor

[2]A.SRAVAN KUMAR [3]CH.RAKESH

[4]V.SAI KUMAR [5]S.CHANDANA

[1,2,3,4,5]Siddartha Institute Of Technology & Sciences, Narapally, TS, India

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 mostnotable 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 inblockchain-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. Index Terms—Federated Learning, Anomaly Detection, Threat Hunting, Blockchain, Industrial Internet of Things, IIoT, IoT.

1. INTRODUCTION

THE technological trajectory of blockchain makes it a valuable tool in many areas, including healthcare, military, finance and networking, via its immutable andtamperproof 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 smart factories [1]. Blockchain technology advantages lead to its wide adoption in IIoTbased 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 ofblockchain-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, Internet of Things (IoT). There are, however, differences and IP phones. These devices are storing private and between IoT and IIoT in terms of security requirements. While the IoT 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-toconsumer) 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, andsharing data securely. Industrial, critical, and personal data are therefore at risk in such a situation. Blockchain technology can ensure data integrity inside and outside of environments. This would lead to a different threat profilesmart factories through strong authentication and ensure or 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 tousers' needs, especially in an industry setting such as the availability of communication backbones. Despite this, privacy and security issues are significant challengesin IIoT [3], [4]. The probability of fraudulent activity occurring inblockchain-based networks [2], [4] is an important issue. Even though blockchain technology is a other [7], [10]. In addition, FL ensures multiple actors powerful tool, it is not protected from cyber attacks construct robust machine learning models without sharing either. For example, a 51% cyberattack [2] on Ethereum data, addressing fundamental privacy, data security, andClassic, and three consecutive attacks in August of 2020 digital rights management challenges. Considering these [5], which resulted in the theft of over $5M worth of cryptocurrency, have exposed the vulnerabilities of this characteristics, this paper uses an FL-based anomaly- detection framework called Block Hunter capable of blockchain network. Smart factories should protect users'detecting attack payloads in blockchain-based IIoT data privacy during transmission, usage, and storage [4]. networks. 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 arXiv:2204.09829v1 [cs.CR] 21 Apr 2022 IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, 2022 2 users and transactions in a blockchain-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 blockchain. 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 blockchain is a complicated

LITERATURE SURVEY

Through the Industrial Internet of Things (IIoT), a smart factory has entered the booming period. However, as the number ofnodes and network size become larger, the traditional IIoT architecture can no longer provide effective support for such enormoussystem. Therefore, they introduce the Blockchain architecture, which is an emerging scheme for constructing the distributed networks, to reshape the traditional IIoT architecture In this work, they define an anomaly detection system based on a encoder-decoder deep learning model, that is trainedexploiting information extracted by monitoring blockchain activities.

Experiments on complete historical logs of Ethereum Classic network prove the capability of the our model to effectively issue [8]. Not only each block needs to be sent to a central detect the publicly reported attacks.which increases the training time, but also the model requires new block data in the testing phase [8]. In addition to the server, when ML models are frequently updated to respond to new threats and detect anomalies, malicious adversaries can launch causative/data poisoning attacks todegrade 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 itselfinstead 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 best of their knowledge, their approach was the first one that provides a comprehensive and feasible solution to monitor the security of blockchain transactions.

ISSN: 2057-5688

EXISTING SYSTEM

A blockchain-based IoT network security solution leveraging a link- mining tool with anomaly detection capabilities is already inexistence. This innovative tool is designed to enhance the security of blockchain networks bygathering metadata in the formof forks,which represent divergent pathsfrom the blockchain protocol. By analyzing these forks, the tool aims to uncover the semantic interpretation of anomalous pathsand activities, utilizing a measure based onmutual information.

The primary objective of this blockchain- based IoT network security solution is to detect and mitigate potential security threats within blockchain networks. Blockchain technology, known for its decentralized and immutable nature, provides a robust foundation for securing IoT networks. However, as the complexity and scale of IoT deployments increase, so do the potential attack vectors and vulnerabilities.

The link-mining tool utilizes unusualor suspicious activities within the lockchain network. Anomalies can include divergent forks in the blockchain, which may indicate unauthorized modifications or malicious behavior. By collecting metadata associated with these forks, such as transaction details and network activity, the tool can analyze and interpret the anomalies.

The semantic interpretation of anomalous paths and activities is achieved through a measure based on mutual information. Mutual information is a statistical metric that quantifies the degree of dependence between two random variables. By applying this measure to the collected metadata, the tool can uncover meaningful patterns and relationships, thereby aiding in the identification and understanding of anomalous behavior.

By leveraging this blockchain-based IoT network security solution, organizations canenhancethe overall security posture of theirIoT deployments. The link- mining tool's anomaly detection capabilities provide earlywarningsigns of potential threats, enabling proactive response and mitigation.

ISSN: 2057-5688

Furthermore, the semantic interpretation ofanomalous paths and activities offers valuable insights into the natureand intentof malicious actors.

The tool interprets anomalous paths and activities by using a statistical metric called mutual information. Mutual informationquantifies how much two variables depend on each other. By applying this metric to the collected metadata, the tool can reveal meaningful patterns and relationships, helping to identifyand understand abnormal behavior.

In conclusion, the blockchain- based IoT network security solution with a link-miningtool and anomaly detection capabilities represents a significant advancement in securing IoT deployments. By gathering metadata from forks and employing mutual information-based measures, thissolution aids in detecting and understanding anomalous behavior within blockchain networks, thereby bolstering the security of IoT ecosystems.

3.1 LIMITATIONS OF SYSTEM:

The system is not implemented on Cluster-Based Local Outlier Factor. It is not implemented in IIOT

4. PROPOSED SYSTEM

In order to detect anomalies effectively, we employ Federated Learning (FL) as a methodto regularly update our model and obtain a global model. This approach allows us toleverage the knowledge and data fromvarious smart factories, including their unique devices and service providers. Once we have learned about the specific data fromeach factory, we send the model's parametersto a parameter server for aggregation. This aggregation process helps to update and refine our general model.

Federated Learning enables us to harness thecollective intelligence of multiple smartfactories without directly accessing their sensitive data. By sending only the model's parameters to the parameter server, we maintain data privacy and confidentiality. The parameter server then performs the crucial task of aggregating the information from all participating factories, ensuring thatour general model reflects the combined knowledge of the entire network.

ISSN: 2057-5688

This iterative process of FL ensures that our anomaly detection model remains up-to-dateand robust. As each smart factory contributes its insights, the global model learns from the diverse range of data and experiences. The aggregation of parameters from multiple factories helps to improve the overall accuracy and effectiveness of our anomaly detection capabilities.

By utilizing Federated Learning and the parameter server, we establish a collaborative framework that empowers smart factories to collectively enhance their anomaly detection capabilities. This approach allows us to continuously update and refine our globalmodel, leveraging the rich and diverse data from various factories while respecting privacy concerns. With each iteration, our anomaly detection system becomes more accurate and reliable, helping to ensure thesmooth operation and security of smart factories in an increasingly interconnected world.

a. ADVANTAGES OF PROPOSED SYSTEM

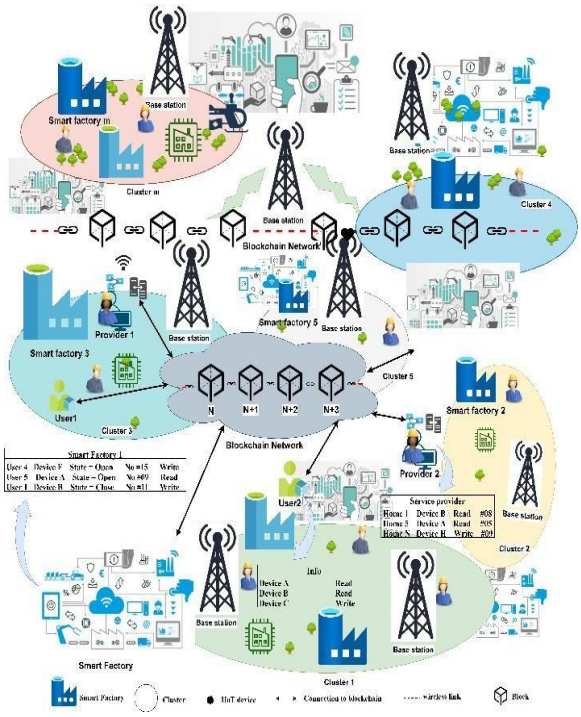
The federation construction involves selecting a subset of smart factory members,forming a cluster, to receive the model locally. These clusters then engage in decentralized training, updating their modelsusing their own local data. This approach ensures data privacy and security.

Finally, the model accumulationprocess collects and merges the data models from the clusters, avoiding the need to individually send and integrate data from the federation to the server. This methodology enables efficient collaboration and knowledge sharing while maintaining confidentiality and minimizing data transfer.

5. SYSTEM ARCHITECTURE

Presents a detailed overview of the proposed blockchain-based IIoT network for smart factory applications. This cluster-based architecture combines users, basestations, WiFi, service providers, andsmart factories connected to the blockchain network. Smart factories include several smartconnected devices. The service provider can collect sensor data in smart factories and use them based on their applications and services. In addition, Fig. 1 illustrates therelationship between the peers in terms of information between the factory and its smart devices.

ISSN: 2057-5688

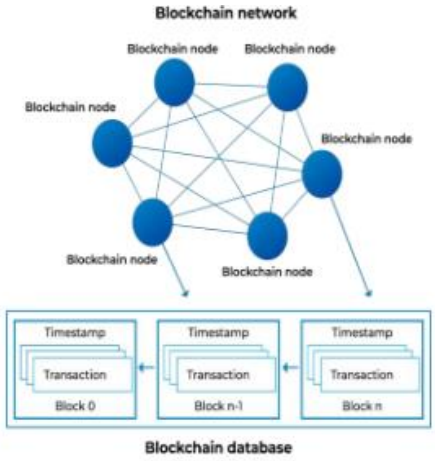


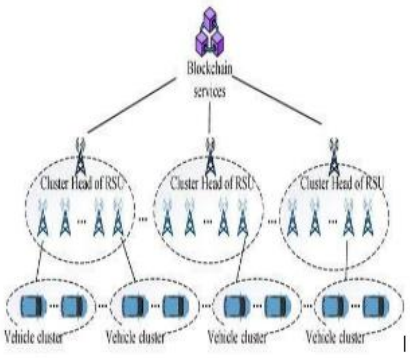
A transaction represents the exchange of sensitive factory information between parties during working in the blockchain network. There are several inputs and outputs in a transaction. Blocks consist of a list oftransactions, a reference to the previous block, and a hash. Every block is made up of transactions that the block creator, referred to as the miner, has accepted into its memory pool from the previous block. Considering rigid industrial standards that should be followed when designing and implementing smart factories, it is practical to assume that the functionality of smart factories in each cluster is the same. Overview of the blockchain-based IIoT network for smart factories Detecting anomalous activitiesis 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. We provide the details of implementing the Block Hunter framework in the following sub- sections

Blockchain Network : A blockchain network is a decentralized and distributed digital ledger that securely recordsand verifies transactions across multiple nodes or computers. It operates on a consensus mechanism where participants agree on the validity of transactions before they are added to the

ISSN: 2057-5688

blockchain. Each transaction is cryptographically linked to the previous one,forminga chain of blocks, hence the name "blockchain." This technology provides transparency, immutability, and security, making it suitable for various applications such as cryptocurrencies, supply chain management, smart contracts, andmore.



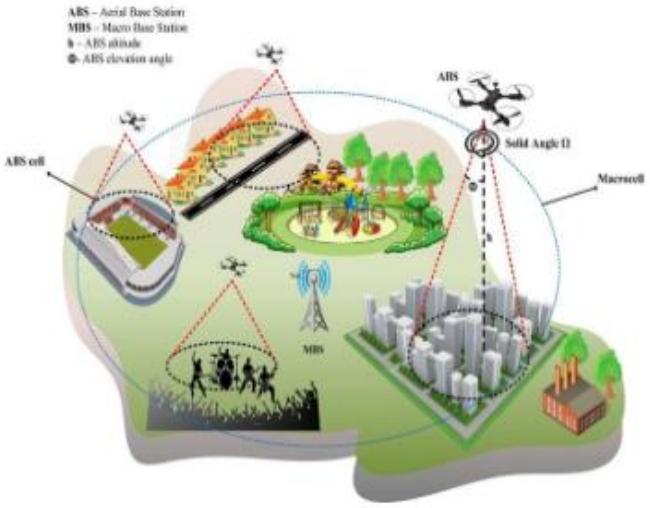


Clusters : In the context of a blockchain network, clusters refer to groups or subsets of nodes or participants that are interconnected and share a common purposeor objective.

These clusters can be formed based on various criteria such as geographical proximity, industry sector, or specific functionalities. Clusters in a blockchain network can collaborate and communicatewith each other to perform specific tasks, validate transactions, or collectively reachconsensus on the state of the blockchain, enhancing the efficiency and scalability ofthe network.

ISSN: 2057-5688

Smart Factories : A blockchain-based IIoT(Industrial Internet of Things) network for smart factories involves integrating the principles of blockchain technology with the infrastructure of IoT devices in a factory setting. This network enables secure and transparent communication, data sharing, and automation among various smart devices within the factory ecosystem. By leveraging blockchain's decentralized and immutable nature, the network enhances data integrity, traceability, and trust among stakeholders, leading to improved operational efficiency, supply chain management, and overall productivity in smart factory environments.



Base Station: In a blockchain-based IIoT network for smart factories, a base station serves as a central communication hub. It acts as a gateway between the smart factory devices and the blockchain network. The base station facilitates the transmission of data collected from sensors and devices within the factory to the blockchain for processing and verification. It also enables the distribution of data and information fromthe blockchain network back to the devices, allowing for secure and decentralized communication.

The base station plays a crucial role in integrating the smartfactory's operations with the blockchaininfrastructure.

6. OUTPUT SCREENS

7. CONCLUSION

In this paper, we developed the Block Hunter framework to hunt anomalies in blockchain- based IIoT smart factories using a federated learning approach. Block Hunter uses a cluster-based architecture to

reduce resources and improve the throughput of blockchain- based IIoT networks hunting. The Block Hunter framework was evaluated using a anomalies. We also examined the impacts ofblock 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 hunterlike framework would be an interesting future research work. Furthermore, designing and applying IIoT- related blockchain networks with differentconsensus algorithms would also be worth investigating in the future.

8. FUTURE SCOPE

Using generative adversarial networks (GAN) to design and implement a block hunter-like framework: This would be an interesting future research direction. Exploring the application of GANs to enhance the effectiveness of anomaly detection in the Block Hunter framework can be pursued. Designing and applying IIoT-related blockchain networks with differentconsensus algorithms: Investigating the impact of different consensus algorithms on the performance and security of IIoT-relatedblockchain networks would be worth exploring in the future. This could lead to insights into selecting the most suitable consensus algorithms for specific IIoT scenarios. variety of machine learning algorithms (NED, IF, CBLOF, K-means, PCA) to detect

9. REFERENCES

[1] J. Wan, J. Li, M. Imran, D.Li, and F. eAmin, "A blockchain-based solution for enhancing security and privacyin 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 anomalydetection," Consiglio Nazionale delle Ricerche, Istituto di Calcoloe 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 applicationfor smart building system management," in Real-Time Data Analyticsfor 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 transactionsigning including
personalized anomaly detection," Sensors,vol. 20, no. 1, p. 147, 2020.

[5] A. Quintal, "Veriblock foundationdiscloses 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 preprintarXiv: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 droneauthentication," Ad Hoc Networks, p. 102574, 2021.

[10] D. Preuveneers, V.Rimmer, I.Tsingenopoulos, J. Spooren, W.Joosen, and E. Ilie-Zudor, "Chained anomalydelearning: 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 smartcities," Computer Standards & Interfaces, vol. 76,p. 103517,2021.

[12] L. Tseng, X. Yao, S. Otoum, M. Aloqaily, and Y. Jarar 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 basedmonitoring systemfor enforcing wastewater reuse," in 2019 10th InternationalConference on Computing, Communication and

ISSN: 2057-5688

NetworkingTechnologies (ICCCNT).

IEEE, 2019, pp. 1–7.

[15] S. Sayadi, S. B. Rejeb, and Z. Choukair,"Anomaly detection model over blockchain electronic transactions," in 201915th International Wireless Communications & Mobile Computing Conference (IWCMC). IEEE, 2019, pp. 895–900.