Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

BLOCK HUNTER: A CYBER THREAT DETECTION SYSTEM ON THE BLOCKCHAIN WITH POOLING LEARNING FOR IIOT NETWORKS

[#1]SAHITHYA MOGILOJU,
[#2] B.ANVESH KUMAR, ***Associate Professor,***
[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

ABSTRACT: The Industrial Internet of Things (IIoT) is a powerful Internet of Things (IoT) application that transforms industry development by boosting open communication between different entities such as hubs, manufacturing facilities, and packaging facilities. The IIoT can more efficiently analyse obtained data by incorporating data science approaches, which current IIoT systems lack due to their distributed nature. Anomalies and assaults on networks pose a serious security risk for IIoT. In this study, a coordinator IoT device is chosen to calculate the trust of IoT devices in order to prevent fraudulent devices from joining the network. Furthermore, implementing a blockchain-based data paradigm promotes data transparency. The proposed system's effectiveness is completely and meticulously verified using MATLAB against a range of security parameters, including attack strength, message tampering, and false authentication likelihood. The simulation findings show that the proposed strategy increases IIoT network security by effectively identifying hostile network threats.

Keywords—*Industrial Internet-of-Things (IIoT), Blockchain, Security, Secure IoT Devices, Trust Management*

1. INTRODUCTION

Today, a company's success and bottom line are dependent on the methods it uses to gather and analyze financial information. As data science and other related fields advance, more opportunities arise for this technology to expand. Statistics from 2016 suggest that there are over 6 billion Internet-enabled gadgets in use today, each contributing to a daily data output of 2.5 quintillion bytes [1].

In most cases, gadgets' real-time data collection and analysis were useless. Innovative Internet of Things (IoT) and smart objects/sensors that cooperate to suit user needs have made it possible for these devices to communicate with one another. The goal of the emerging subject of data science is to find meaningful patterns and insights in massive datasets by the application of rigorous scientific methods, algorithms, procedures, and systems. The goal of data science in the Internet of Things (DS-IoT) is to make data collection and processing faster, more realistic, and more scientific. Sensors worn by workers in the transportation, cyberphysical systems, and medical fields can preserve records and provide production data thanks to the interoperability enabled by the DS-IoT.

Due to its importance in the IoT, the DS-IoT paradigm [2] has gained recognition for enabling devices to generate their own data. performance over time [5, 6]. Smart cities, e-healthcare, intelligent transportation, and Industrial IoT (IIoT) are all examples of IoT-based applications that aim to improve decision-making by facilitating the efficient management of a variety of physical objects crucial to scaling experiments [7, 8]. The Industrial Internet of Things (IIoT) is a crucial use of IoT since it monitors and reports on all activities in the industrial sector to promote its development [8]. The Internet of Things (IoT) is a system that connects various devices together to share information [9, 10].

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

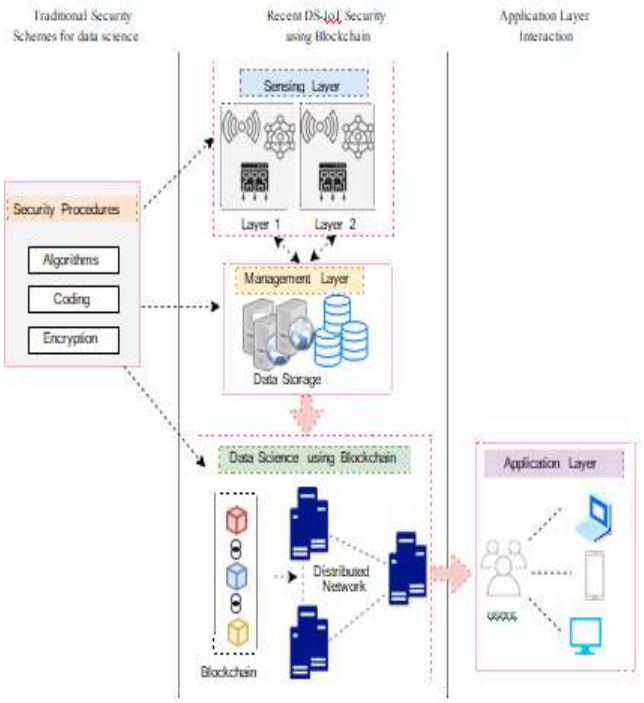

Fig. 1: DS-IoT Blockchain in Industrial IoT

Despite the many advantages of the DS-IoT approach, enterprises are hesitant to implement IoT devices [11] due to security concerns. Within typical industry parameters, a rogue IoT device can degrade network performance by preventing trustworthy IoT devices from providing trustworthy data or by tampering with communication data. Some open-source ciphers still contain vulnerabilities and can be attacked, but they are under regular scrutiny from a large number of users, rendering any negative alterations made by centralized or external entities ineffective [12]. In most commercial settings, the interoperability and dependability of all smart devices is taken as a given. Unfortunately, malicious devices (MD) are capable of hacking into IoT products. Differentiating between trustworthy and malicious DS-IoT gadgets could be crucial for establishing an environment conducive to open communication. For the sake of security and public confidence, it is crucial that data owners be made aware of any changes made to their information as soon as possible [14]. The use of a blockchain has recently been proposed as a safeguard against data tampering in the future of smart devices. As can be seen in Figure 1, a blockchain network stores a chain of blocks made up of data acquired by IoT devices throughout the production and distribution of a product.

Clear and effective data analysis and management are now possible thanks to blockchain technology. Data modifications made by each user are recorded in a blockchain. Through the development of IIoT, automated systems can be networked together to deal with events simultaneously, enabling prompt responses and covert surveillance. The data science method guarantees efficient data collection, processing, and management in IIoTs. Although DS-IoT has numerous applications in industry, many businesses and organizations are still wary of adopting it. The expensive price of centralized cloud and server infrastructure [15–17] discourages widespread adoption of this IoT alternative. The author was unable to find any evidence that IIoT employs DS-IoT security via blockchain in the cited works. Whether it's a boiler's temperature, a product's production history, or its shipping details, IoT devices in an IIoT setting transmit very sensitive data. The IIoT network's top priority must be to implement security by design. Also, the IIoT network is vulnerable to attack if malicious nodes can alter data from IoT devices. This has me thinking about the best way to design a network infrastructure to keep information safe from intrusion while still allowing devices to exchange data.

2. RELATED WORK

Research in data science and blockchain technology has been conducted to discover methods of IIoT network security. To investigate data processing issues in industrial big data, Yan et al. [18] provided distinctive structure multi source data for diverse contexts. Using a variety of data sets from the same company, the efficacy of this strategy is demonstrated. The authors examined the storage, processing, and utilization of data in the context of smart devices for data-driven business processes. They failed to consider the possibility of unauthorized access to the data and the means by which it may be protected. In

addition, Wang et al. [19] developed a state-of-the-art industrial data processing system that has a broad comprehension of operations common in manufacturing, including distributed access and storage, stream and bulk data processing, and real-time regulation. It has been proven in [19] that the Internet of Things (IIoT) involves much more evaluating, correlating, and integrating of massive amounts of data than do standard data processing systems. However, issues including storage, communication via intermediate nodes, and expensive transmission can result from creating such a massive data set. That's why scientists are still scratching their heads over how to ensure data is transmitted safely through trusted intermediaries. For many IIoT companies, blockchain now represents the best hope for incorporating decentralization, trust, privacy, and security into their operations. To ensure the security of data transmission between IoT devices, S. Yu et al. [20] devised a blockchain-based method of sending data with low transaction costs and high economic transfer value. Methods such as distributed network architecture, the consent algorithm, and intelligent device mapping were used to figure out the decentralized autonomy of smart devices. Privacy and security issues with IoT devices were discussed in a paper written by Y. Yu et al. [21]. Confirmed data transmission for payments, decentralized processes, and confirmed scalability are just a few of the advantages of the blockchain-enabled IoT architecture. The phenomena is further supported by concrete Ethereum solutions that exhibit blockchain's potential applications in the Internet of Things. However, the study does not specify whether hackers may utilize a public or private blockchain to launch attacks on IoT gadgets.

To safeguard individual privacy in the IoT industry, Oh et al. [22] propose a protocol for exchanging information. To determine the market's viability, the authors employed the Nash equilibrium to maximize profits for all participants. Hasan et al. [23] developed an interplanetary file system for IoT devices to transmit and store information. The blockchain-based solution the authors propose has been thoroughly tested for security via the creation of smart contracts, algorithms, diagrams, and procedures for implementing the system. The authors have demonstrated that their alternative approach is superior to the status quo. Meaning was the driving force behind Lam et al.'s [24] introduction of a decentralized autonomous orchestration and configuration solution. The proposed approach was employed to transmit data over the cloud in an IIoT scenario during planning and production, and the results were analyzed.

Many studies have proposed solutions to ensure IIoT networks have a decentralized, transparent, and secure structure, but relatively few have examined the many methods by which intruders attempt to disrupt or exhaust network resources. Furthermore, the authors did not employ trust-based methodologies to validate the integrity of blockchain-based IIoT network nodes, data storage, or processing operations.Because of their potential impact, data science methods in IoT have been the subject of extensive research. Additionally, there has been scant research into blockchain's security in the industrial IoT. The IIoT network can become more reliable and effective at evaluating industrial data if blockchain technology and data science are integrated into it. Consequently, this research provides IIoT with a cutting-edge and secure foundation by employing data science and blockchain to identify potential network vulnerabilities. More information regarding our planned structure will be provided in the next section.

3. PROPOSED INDUSTRIAL BLOCKCHAIN FRAMEWORK

We analyzed an IIoT network that contained both trustworthy and malicious nodes to demonstrate the efficacy of our approach. A system model is employed to support the suggested framework. To guarantee the security of data analysis in a DS-IIoT environment, a blockchain is integrated into

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

the IIoT network. Finally, a mathematical model is constructed to evaluate the performance of the network. Using blockchain technology, CU can construct control systems and data-sharing systems to address issues including decentralized information circulation, internal information access control, and privacy during data exchange between various parties. In a blockchain-based system, as depicted in Figure 2, all users may view and track the history of all documents that have ever been created by any given business. If a data record or change to a record was produced maliciously, this would be immediately apparent using blockchain technology.

Fig. 2: Data Model of DS-IIoT using Blockchain

Algorithm 1: Execution of Proposed IIoT Framework

Assumption: $Count_{threshold}$ = 50%
Input: (1) Network with 'n' IDs, (2) Among them one CID is elected, and (3) 'm' number of MD's
Output: ID identified as either legitimate or malicious
The CID selection is based on ST, energy level and MC.
CID maintains a table having ID id, ID address, routing information, CID id, ST and TF of each ID to identify MD. Upon the emergence, the NID is identified as MD else legitimate.
if *(ID is NID)* **then**
  CID allows first five assumptions and;
  Compute TF();
  Compute MC();
  Blockchain record ();
  The information of each record corresponding to ID is stored in the database with its current and previous hashes.
else
  ID is elected as MD
end

4. RESULTS

What happens to the actual devices on the network is depicted in Figure 4 when an IoT device is compromised. The lack of a trust-based structure in IoT devices makes them a soft target for hackers. To prevent fake devices from joining the network, the existing method relies on a trust-based system to authenticate new members. This reduces the potential for harm when hacking an IoT device.

The phenomenon proposed, on the other hand, is more productive because CID identifies TF based on their intrinsic behaviors. Like Figure 6, Figure 7 demonstrates that the hypothesized phenomena improves when compromised miners are considered. Attackers might easily switch miners during network setup, however this doesn't happen because miners are selected based on their TF. The following are more restrictions on this publication. One can't tell how well the proposed approach for data exchange in IIoT networks using blockchain technology performs just by comparing security measures to any current

method. No authors have, to our knowledge, developed blockchain-based data science methodologies for use in the Industrial Internet of Things. Second, the block verification procedure could delay validation, which would increase the likelihood of more network security threats, meaning the proposed system cannot make a smart judgment while transferring information in real time.

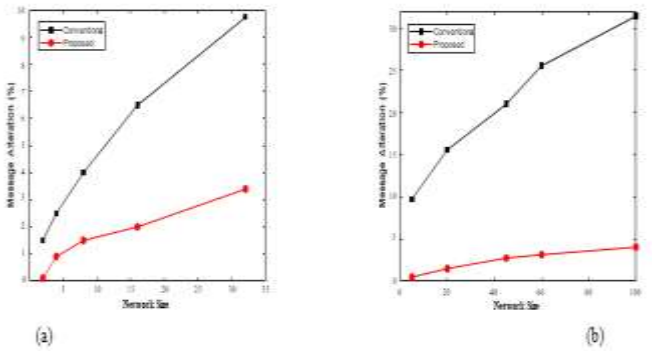

Fig. 3: Message Alteration for (a) Small Network (b) Large Network

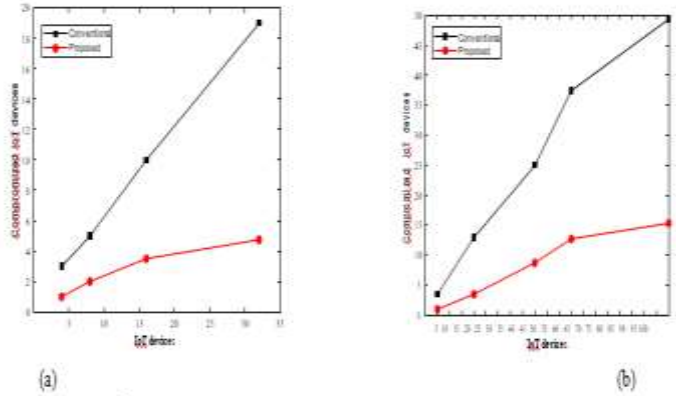

Fig. 4 Compromised IoT deivces for (a) Small Network (b) Large Network

5. CONCLUSION

This research proposes a secure blockchain- and trust-based architecture to address the multi-tiered issues that MDs create in IIoT systems. The proposed paradigm determines whether or not an IoT device is authorized by computing its Trust Factor (TF) via a designated Coordinator IoT Device (CID). In order to monitor industry-wide activity and prevent unauthorized changes to the local database, a blockchain-based data model is employed behind the scenes. The methodology has been extensively tested across a variety of network sizes and assessment criteria. Our proposed design outperforms the network without a blockchain in simulations in 91% of all cases.

REFERENCES

[1] A. Karpatne, G. Atluri, J. H. Faghmous, M. Steinbach, A. Banerjee, A. Ganguly, S. Shekhar, N. Samatova, and V. Kumar, "Theory-guided data science: A new paradigm for scientific discovery from data," IEEE Transactions on Knowledge and Data Engineering, vol. 29, no. 10, pp. 2318–2331, 2017. doi:10.1109/TKDE.2017.2720168.

[2] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things Based Smart Cities: Recent Advances and Challenges," IEEE Communications Magazine, vol. 55, no. 9, pp. 16–24, 2017. doi: 10.1109/MCOM.2017.1600514.

[3] H. Oh, S. Park, G. M. Lee, H. Heo, and J. K. Choi, "Personal data trading scheme for data brokers in iot data marketplaces," IEEE Access, vol. 7, pp. 40120–40132, 2019. doi:10.1109/ACCESS.2019.2904248.

[4] P. A. Merolla, J. V. Arthur, R. Alvarez-Icaza, A. S. Cassidy, J. Sawada, F. Akopyan, B. L. Jackson, N. Imam, C. Guo, Y. Nakamura, et al., "A million spiking-neuron integrated circuit with a scalable communication network and interface," Science, vol. 345, no. 6197, pp. 668–673, 2014. doi:10.1126/science.1254642.

[5] C.-X. Wang, F. Haider, X. Gao, X.-H. You, Y. Yang, D. Yuan, H. M. Aggoune, H. Haas, S. Fletcher, and E. Hepsaydir, "Cellular architecture and key technologies for 5g wireless communication networks," IEEE communications magazine, vol. 52, no. 2, pp. 122–130, 2014. doi:10.1109/MCOM.2014.6736752.

[6] E. Bertino and N. Islam, "Botnets and internet of things security," Computer, no. 2, pp. 76–79, 2017. doi:10.1109/MC.2017.62.

[7] L. Zhou, D. Wu, J. Chen, and Z. Dong, "When computation hugs intelligence: Content-aware data processing for industrial iot," IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1657–1666, 2017. doi:10.1109/JIOT.2017.2785624.

[8] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial

iot: Blockchain system with credit-based consensus mechanism," IEEE Transactions on Industrial Informatics, 2019. doi:10.1109/TII.2019.2903342.

[9] F. Al-Turjman and S. Alturjman, "Context-sensitive access in indus- trial internet of things (iiot) healthcare applications," IEEE Transac- tions on Industrial Informatics, vol. 14, no. 6, pp. 2736–2744, 2018. doi:10.1109/TII.2018.2808190.

[10] J. Wan, J. Li, M. Imran, and D. Li, "A blockchain-based solution for enhancing security and privacy in smart factory," IEEE Transac- tions on Industrial Informatics, vol. 15, pp. 3652–3660, June 2019. doi:10.1109/TII.2019.2894573.

[11] J. A. Shamsi and M. A. Khojaye, "Understanding privacy violations in big data systems," IT Professional, vol. 20, no. 3, pp. 73–81, 2018. doi:10.1109/MITP.2018.032501750.

[12] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, and D. Chen, "Enhancing cloud-based iot security through trustworthy cloud service: An integra- tion of security and reputation approach," IEEE Access, vol. 7, pp. 9368– 9383, 2019. doi:10.1109/ACCESS.2018.2890432.

[13] H. Moosavi and F. M. Bui, "Delay-aware optimization of physical layer security in multi-hop wireless body area networks," IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1928–1939, 2016. doi:10.1109/TIFS.2016.2566446.