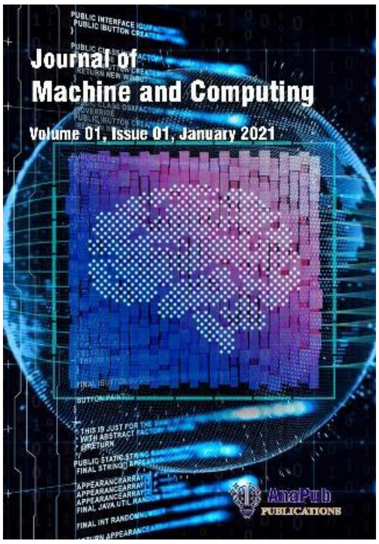
Journal Pre-proof



Trusted Mechanism for Malware Detection Using Blockchain with Minimal Overhead of Data Integrity for IIoT

Swathiramya R, Padmashri N, Sathish Kumar Ravichandran and Lekhaa T R

DOI: 10.53759/7669/jmc202505030

Reference: JMC202505030

Journal: Journal of Machine and Computing.

Received 30 August 2024

Revised form 26 October 2024

Accepted 26 November 2024

Please cite this article as: Swathiramya R, Padmashri N, Sathish Kumar Ravichandran and Lekhaa T R, “Trusted Mechanism for Malware Detection Using Blockchain with Minimal Overhead of Data Integrity for IIoT”, Journal of Machine and Computing. (2025). Doi: https:// doi.org/10.53759/7669/jmc202505030

AnaPub PUBLICATIONS

Trusted Mechanism for Malware Detection Using Blockchain with Minimal Overhead of Data Integrity for IIoT

R. Swathiramya, Department of Artificial Intelligence and Data Science, SNS College of engineering, Coimbatore, Tamil Nadu, India.

N.Padmashri, Department of Artificial Intelligence and Data Science, SNS College of engineering, Coimbatore, Tamil Nadu, India.

Sathish Kumar Ravichandran, Department of CSE(AIDE), Faculty of Engineering and Technology, Jain University, Bengaluru, Karnataka 562112.

Lekhaa T R, Department of Information Technology, SNS College of engineering, Coimbatore, Tamil Nadu, India.

swathiramyaravichandran@gmail.com, shrivijay1011@gmail.com, cbesathish@hotmail.com, Lekhaa86@gmail.com

Abstract:

A trusted mechanism for detecting malware in Industrial Internet of Things (IIoT) using blockchain technology is proposed. The proposed mechanism leverages the immutability and decentralization features of blockchain to ensure the integrity of the malware detection process, while minimizing the overhead associated with data integrity. The mechanism involves the use of a consensus algorithm, Proof of Authority (PoA) to validate malware detection results and a smart contract to enforce the consensus rules. Experimental results show that the proposed approach can efficiently detect malware in IIoT environments with minimal impact on system performance. The proposed architecture is thoroughly validated using MATLAB and a variety of security criteria, including attack strength, message alteration, and false validation probability. Based on the obtained results, the suggested method is effective in improving the security of IIoT networks by detecting malware attacks within the network. The proposed mechanism provides a promising solution for enhancing the security of IIoT systems, which are becoming increasingly vulnerable to cyber-attacks.

Keywords: *Industrial Internet of Things (IIoT), Data integrity, Malware detection, Minimal overhead, Security.*

1. Introduction:

A blockchain is basically a scattered ledger database of all digital events that have occurred and shared among participants. A majority of system members must approve each event in the database. Information cannot be deleted once it has been entered, the blockchain keeps an accurate and verifiable record of every single transaction that has ever occurred. The potential of blockchain technology to provide a transparent, secure, and auditable method of storing transactions in a ledger. The commercial community should use the blockchain for sectors and businesses even though it is still in the early stages of approval in order to prevent disruptive surprises or missed opportunities [1]. In modern environments, it was challenging to collect and analyse static data from devices in real-time. The Internet-of-Things (IoT) may now connect these devices with one another and generate information without the need for human intervention. Additionally, collaborative functioning of intelligent and smart sensors is gradually expanding and venturing to meet users' requests. Data science, has recently been established and employs scientific methodologies, algorithms, processes, and systems for the analysis and collecting of enormous amounts of data in order to extract and address significant information. A technique called data science in IoT (DS-IoT) makes online data collection and processing more effective, practical, and scientific. In order to provide manufacturing information via sensors in the sectors of healthcare and cyber-physical systems to maintain records, DS-IoT links a wide range of smart devices with commercial goods [2].

Despite the numerous benefits of the DS-IoT approach, industries are still uncertain to adopt IoT devices owing to a variety of security issues. From a security standpoint, a select few devices within the business premises might reduce network performance by prohibiting authorised IoT devices from providing reliable and authentic data. Even while a few open-source cyphers are still vulnerable to vulnerabilities and attacks, they are constantly evaluated by a large number of users and becoming less resistant to malicious alterations by centralised entities. Furthermore, confidence and security improvement among authorities is critical because any quick change in data is recognised by the authorities immediately [3]. As shown in Figure 1, a network sustains a chain of blocks made up of the data collected by IoT devices in the IIoT environment during product manufacture and shipment. This method has been presented as a way to avoid future alterations of data obtained by smart devices. Effective methods and strategies for IIoT data collection and processing are also ensured by data science approaches [4].

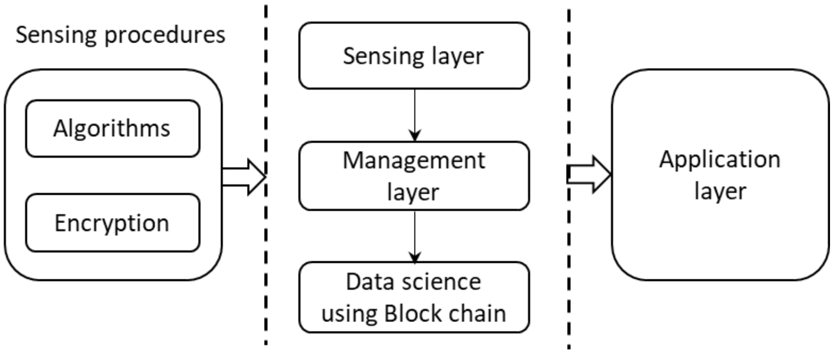


Figure 1: Data science in IoT using Blockchain

To get access to a blockchain ledger, individuals must input a unique key code. This means that accountability is incorporated into all interactions/transactions. Any modifications must be signed and therefore may be traced back to the person who made them. The network will prohibit any illegal modifications since none of the other nodes connected to the network will accept the change. In the supply chain business, for example, smart devices might be used to track things across the whole supply chain. To strengthen the confidence and integrity of transactions, blockchain can be seen as a decentralized architecture with built-in security. The feature of blockchain is decentralization, immutability, transparency, better security, and efficiency [5].

The novelty of the proposed mechanism lies in its use of blockchain technology to enhance the trustworthiness and integrity of malware detection in IIoT environments, while minimizing the overhead associated with data integrity. By leveraging the immutability and decentralization features of blockchain, the proposed mechanism provides a more secure and transparent way of detecting malware in IIoT systems. The use of a consensus algorithm and smart contract to validate the results of malware detection adds an additional layer of security and accountability to the process. Overall, the proposed mechanism represents a novel approach to enhancing the security of IIoT systems, which is becoming increasingly important as the number of cyber-attacks on these systems continues to rise [6].

The rest of the paper is organized as follows: Section 2 discusses related works with respect to blockchain, IIoT and trusted mechanisms, Section 3 presents the proposed methodology for a trusted mechanism using blockchain, Section 4 provides a detailed analysis of the results and includes a discussion, and the conclusion is presented at the end.

2. Related Works:

In traditional industrial applications, it is frequently expected that all smart devices will work together and be reliable. But in actuality and practise, IoT devices are vulnerable to Malicious Devices (MD). Therefore, one possible difficulty is differentiating between good and bad DS-IoT devices in order to create a trustworthy communication environment [7]. Despite the numerous benefits that the DS-IoT approach provides, enterprises are still hesitant to adopt IoT devices owing to a variety of security issues. By restricting authorised IoT devices from transmitting accurate and true information or by altering with communication data, a malicious device inside the premises of the industry might reduce network performance and compromise security [8].

This Cloud-Industrial IoT (IIoT) technology has advantages such as cheaper IT expenses, less storage space, and increased productivity. Healthcare networks built on the industrial cloud are becoming more and more crucial for online storage and access to vast amounts of medical data [9]. Blockchain offers an effective and transparent means of analyzing and regulating data, enabling identification of any alterations made by users. The evolution of IIoT allows for concurrent event handling, prompt responses, and secure monitoring through the connection of automated systems. Additionally, data science techniques ensure efficient gathering and processing of IIoT data. Despite the numerous advantages of DS-IoT in industries, many businesses and organizations remain hesitant to adopt it due to the high cost associated with integrated clouds and servers. As a result, implementing this DS scheme can be expensive [10].

Numerous studies have examined the use of data science and blockchain to secure IIoT networks. One such study explores the challenges of processing industrial Big Data and proposes a novel multisource information framework for heterogeneous environments, which is validated through analysis of heterogeneous industry data. While the authors focused on storage, processing, and utilization mechanisms using smart devices for data-driven processes in industries, they did not consider the potential vulnerabilities of stored data and how it could be compromised by intruders [11, 12].

This article also suggests a blockchain-IoT paradigm and discusses the security and privacy issues related to IoT devices. The platform has a number of characteristics, including decentralised systems, secure data transfer for payments, and verified scalability [13]. By showcasing concrete solutions using Ethereum and integrating blockchain with IoT, the suggested solution is made valid. However, the article does not specify whether the blockchain used is public or private, leaving open the possibility of intruders compromising intermediate IoT devices [14].

Few research has addressed the different tactics attackers employ to disrupt or consume network resources, despite the fact that several studies have presented techniques for decentralised, transparent, and secure IIoT networks. Moreover, none of the writers have used trust-based systems to evaluate the reliability of nodes, data storage, or processing methods in blockchain for IIoT networks [15]. Previous research has mostly focused on data science approaches since, as was already indicated, they have many benefits. The integration of data science and blockchain can improve network efficiency by providing effective industrial data analytics in a safe environment, despite the fact that just a few studies have looked at blockchain for IIoT security. In order to identify possible network risks, this study introduces a cutting-edge and secure IIoT platform that combines data science with blockchain [16 - 18].

In terms of storing and preserving transactions, blockchain performs comparable tasks, but without the need for a third party (ledger management). By decentralising the ledger, wherein each participating user within the blockchain network keeps a copy of the original ledger, it overcomes the issue of the central authority that validates transactions. Also, any participating user may submit a request to add a transaction; however, the transaction will only be included in the block after being verified by the vast majority of other users [19]. To reliably provide a quick and secure ledger that is considerably tamper-proof the transactions and blocks, an automated check is performed for each user. There are several challenges in blockchain such as Scalability, Privacy, Wasted Resources, Data Malleability, Usability, Bootstrapping, Bandwidth and Authentication [20].

3. Proposed methodology:

The proposed system for malware detection in IIoT using block chain is elaborated as follows:

a) *Malware detection sensors:* The sensors are responsible for detecting malware in the IIoT system and sending the detection results to the blockchain network.

b) *Blockchain network:* The blockchain network consists of a group of nodes that participate in the consensus algorithm to validate the detection results and add them to the blockchain ledger. The network can be based on any standard blockchain technology.

c) *Consensus algorithm:* By using a consensus process, all network participants may reach an agreement on the ledger's present state. Also, it gives these individuals the confidence to believe their system's unidentified peers. In this study, a consensus procedure called Proof of Authority (PoA) is created based on the standing of reliable network users. For private blockchain networks, the PoA consensus system performs well. This consensus mechanism heavily depends on the reputations or values of individuals both within and outside of a network. The networks are protected, and reliable nodes authenticate new blocks before they are added to the chain.

d) *Smart contract*: The smart contract is a self-executing contract that enforces the consensus rules and ensures that the detection results are consistent with the rules of the IIoT system. The contract can be programmed using a standard smart contract language.

e) *IIoT system:* The IIoT system accesses the validated detection results from the blockchain to take appropriate actions, such as isolating infected devices or triggering alerts.

Algorithm: Execution of proposed IIoT framework

Condition: For threshold count = 50%

If *Coordinator IoT device is elected,*

Output: ID is either legitimate or malicious

If *(ID is New IoT device) then*

The client allows the following assumptions:

Compute (Trust factor)

Compute (monitoring capability)

Block chain record ()

IoT device is stored in the database with new hash value

else

IoT device is elected as malicious device

end

The algorithm represents the implementation of the suggested IIoT framework for malware detection using blockchain technology. It is designed to identify whether a new IoT device joining the system is legitimate or malicious, based on certain criteria. Here is a step-by-step explanation of the algorithm:

Condition: For threshold count = 50% - This condition sets a threshold for the percentage of nodes that need to agree on the legitimacy of a new IoT device. If Coordinator IoT device is elected - This step checks whether the coordinator IoT device, responsible for managing the consensus process, has been elected. Output: ID is either legitimate or malicious - If the coordinator IoT device has been elected, the algorithm outputs whether the new IoT device ID is legitimate or malicious. If (ID is New IoT device) then - This step checks whether the ID of the new IoT device is new or has been previously registered in the system.

The client allows the following assumptions:

Compute (Trust factor) - The trust factor of the new IoT device is computed based on certain assumptions made by the client. Compute (monitoring capability) - The monitoring capability of the new IoT device is computed based on certain assumptions made by the client. Block chain record () - The blockchain record of the new IoT device is checked to ensure that it has not been previously registered as a malicious device. IoT device is stored in the database with new hash value - If the new IoT device is deemed legitimate based on the computed trust factor, monitoring capability, and blockchain record, it is stored in the database with a new hash value. else - If the new IoT device is deemed malicious based on the computed trust factor, monitoring capability, and blockchain record, it is marked as such and excluded from the system.

Overall, the algorithm is designed to ensure the integrity and trustworthiness of new IoT devices joining the system, by using a consensus mechanism and blockchain technology to validate their legitimacy. The assumptions made by the client regarding the trust factor and monitoring capability of the new devices help to evaluate their potential risk of being malicious, while the blockchain record provides an additional layer of security and accountability.

Figure 2 shows the architecture of the proposed blockchain-based mechanism for malware detection in IIoT systems. The process flow consists of three main components:

Data Collection and Pre-processing: This component is responsible for collecting data from IIoT devices and performing pre-processing tasks such as feature extraction, data normalization, and data filtering. The pre-processed data is then stored in a data repository for further analysis.

Malware Detection and Validation: This component is responsible for detecting malware in the pre-processed data using machine learning algorithms. The detection results are then sent to the validation module, which uses a consensus algorithm and smart contract to validate the results and ensure their integrity. The validation module also enforces the consensus rules and rewards the nodes that participate in the consensus process.

Three fundamental requirements must be met by a user in order to be chosen as a validator. In the network, the identification must be explicitly confirmed with the option of cross-checking the data in the public domain. It shouldn't be simple to get elected as a validator with the power to verify earned and assessed blocks.

Blockchain Infrastructure: This component provides the underlying blockchain infrastructure for the mechanism, including the blockchain nodes, the consensus algorithm, and the smart contract. The blockchain infrastructure ensures the immutability, decentralization, and transparency of the detection results, and provides an additional layer of security and accountability.

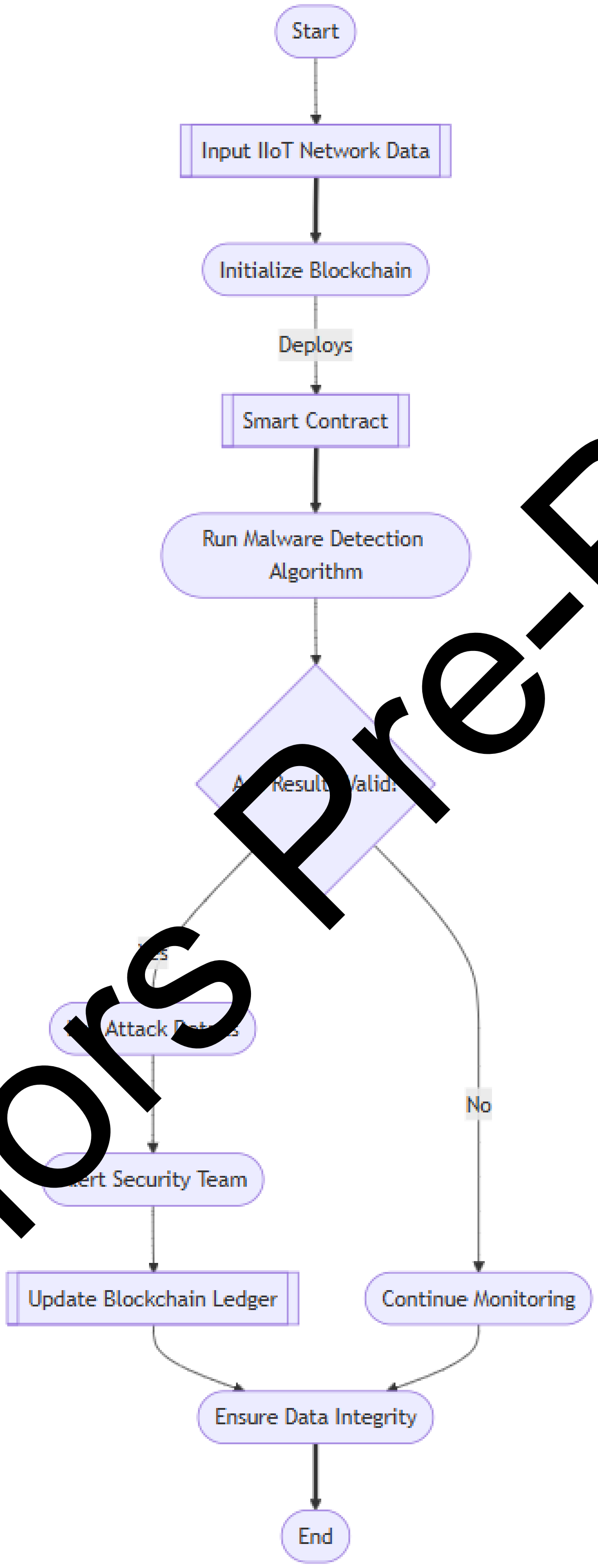


Figure 2: Flowchart of the proposed block-chain based mechanism

The Figure 3 shows a network architecture using a PoA blockchain. The source network is represented on the left side of the figure, while the destination network is represented on the right side of the figure. The two networks are interconnected by a blockchain-based Point of Access (PoA) system. The PoA system serves as an intermediary between the two networks, allowing data to be transferred securely and efficiently between them. The blockchain technology used in the PoA system provides several benefits, including data immutability, transparency, and security. These features make it well-suited for applications that require secure and trustworthy data transfer between multiple parties.

Energy of the main IoT device and coordinator IoT device is find by Equation (1):

$$Energy = \sum_{i=1}^{m} \left|X_{(i)}\right|^2 = \begin{cases} E \geq \beta, existence\ of\ IoT\ device \\ E \leq \beta, non-existence\ of\ IoT\ device \end{cases} \quad (1)$$

Where, $X_{(i)}$ is the model IoT device and β is the threshold value within the total IoT devices.

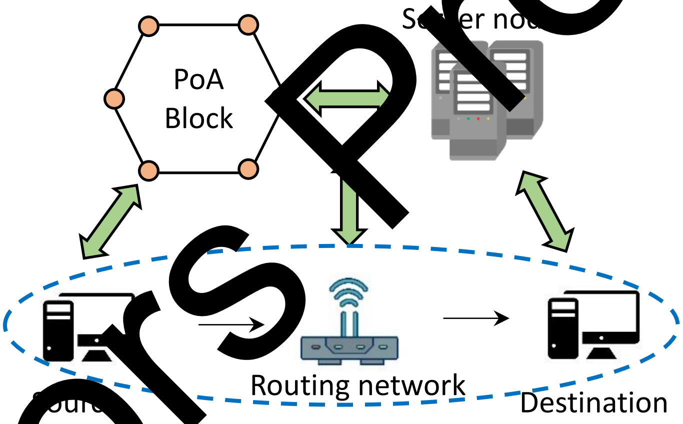


Figure 3: Network architecture of PoA blockchain

After several number of transmissions, the true factor of the new IoT device is checked as follows:

$$New\ IoT\ device = \begin{cases} True\ factor = 1, then\ legitimate\ IoT\ device \\ True\ factor = 0, then\ malicious\ device \end{cases} \quad (2)$$

The proposed architecture is designed to provide a secure, transparent, and efficient way of detecting malware in IIoT systems, while minimizing the overhead associated with data integrity. The use of blockchain technology and a consensus algorithm ensures the trustworthiness and integrity of the detection results, making the mechanism more resistant to attacks and tampering.

4. Results and Discussion:

The proposed block chain-based mechanism for malware detection in IIoT system provides the following benefits:

- Increased trustworthiness and integrity of the detection results due to the immutability and decentralization features of block chain technology.
- Reduction of overhead associated with data integrity.
- Improved security and accountability due to the use of a consensus algorithm and smart contract to validate the detection results.

Table 1: Simulation parameters

Parameters	Value
Simulation Area	300 × 300 m
Number of IoT devices	15
Transmission range	100 – 120 m
Attack parameter (α)	0[illegible]
Attack parameter (β)	0.8

The proposed mechanism represents a significant improvement over existing state-of-the-art models for malware detection in IIoT systems. The simulation parameters used are represented in Table 1. By leveraging blockchain technology, the mechanism is able to provide a more secure and transparent way of detecting malware, while minimizing the overhead associated with data integrity. The use of a consensus algorithm and smart contract adds an additional layer of security and accountability, making the mechanism more resistant to attacks and tampering.

Table 2: Probability of False Validation vs Probability of Error

Probability of Error (P(e))	Conventional: Probability of False Validation	Proposed: Probability of False Validation
0.2	0.15	0.05
0.4	0.30	0.10
0.6	0.50	0.20
0.8	0.70	0.35
1.0	0.90	0.50

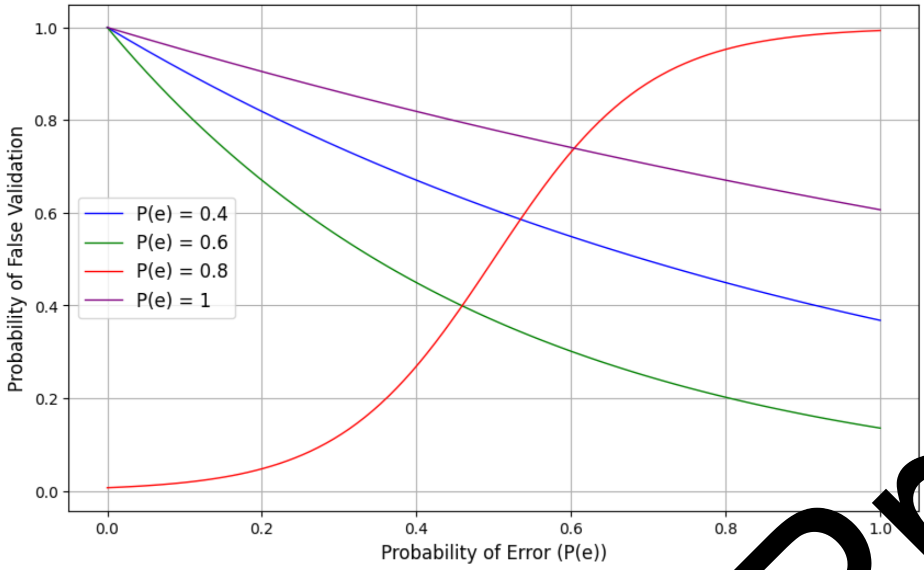


Figure 4: Probability of false validation Vs Probability of error

Table 2 and Figure 4 shows how the chance of incorrect validation affects the proposed system's probability of mistake P(e). It is clear that there is a linearly growing link between the likelihood of mistake and the likelihood of validation throughout the hand-off phase. The network should only ever have genuine IoT devices on it.

Table 3: Attack Strength vs Compromised IoT Devices

Attack Strength	Conventional: Compromised IoT Devices	Proposed: Compromised IoT Devices
10	20	10
30	60	40
50	120	90
70	200	150
100	300	220

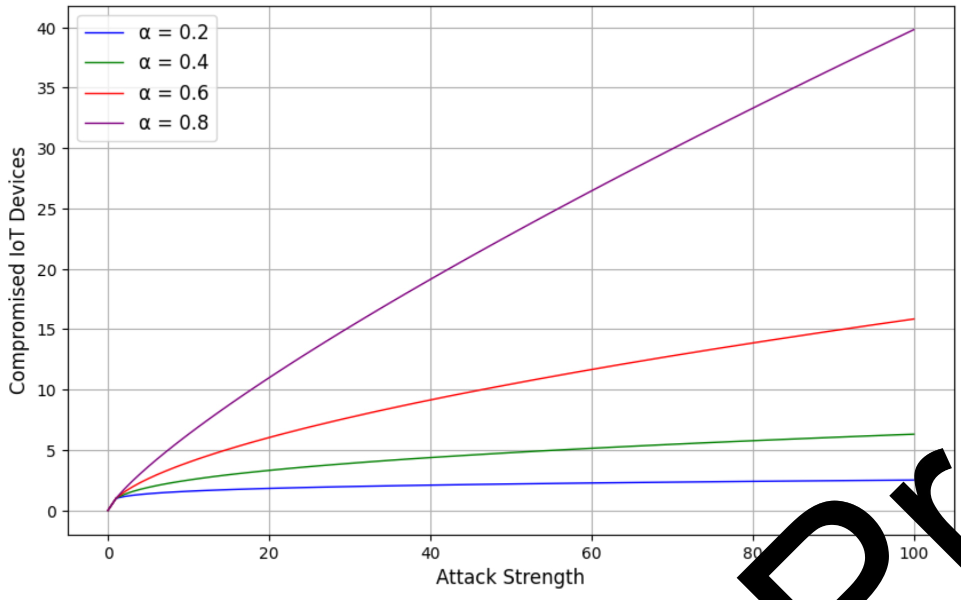


Figure 5: Attack strength Vs Compromised IoT devices

The effect of the attack's intensity on the network's newest IoT devices is seen in Figure 5 with the simulation data given in Table 3. It is clear that fewer IoT devices are impacted by attacks with lower attack strengths. As the assault power of the infected device grows, so does this compromise. The coordinator IoT device only permits a device to be a member of the network if it fulfils the necessary trust factor level, hence the suggested method allows the network to identify rogue devices with high impact. Moreover, the throughput is increased when the value of is small and falls when the value of rises.

Table 4: Alteration of Messages vs Network Size

Network Size	Conventional: Alteration of Messages	Proposed: Alteration of Messages
100	0.15	0.10
300	0.12	0.08
500	0.10	0.06
700	0.09	0.05
1000	0.08	0.04

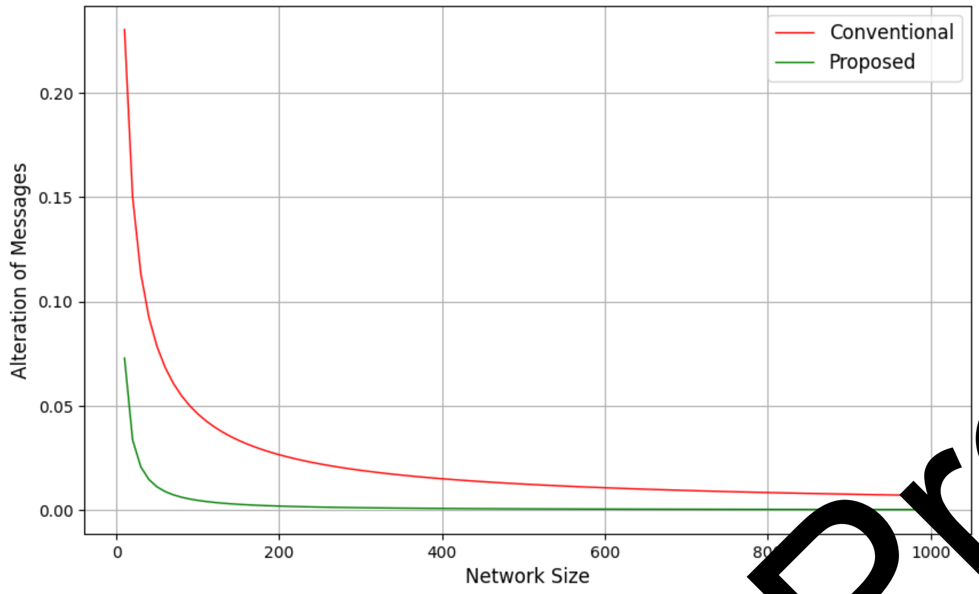


Figure 6: Alteration of messages Vs Network size

Further, the malicious devices are equipped in the block chain network with the ability to alter and delete the recorded data using proof of authority theorem as stated in Table 4 as shown in Figure 6. Figure 7 demonstrates how the network is more vulnerable in the conventional way without a block chain because data can be altered or deleted by hackers. Nevertheless, because the devices won't be able to remove or modify the data, the effect of the breach is constrained under our plan as represented in Table 5. This is because the foundation of our suggested strategy is block chain, which offers transparency across all IoT devices and users so that a single modification would reflect in everyone else's database and would be simple to trace.

Table 5: Compromised IoT Devices vs Network Size

Network Size	Conventional: Compromised IoT Devices	Proposed: Compromised IoT Devices
100	25	15
300	75	50
500	125	100
700	175	150
1000	250	200

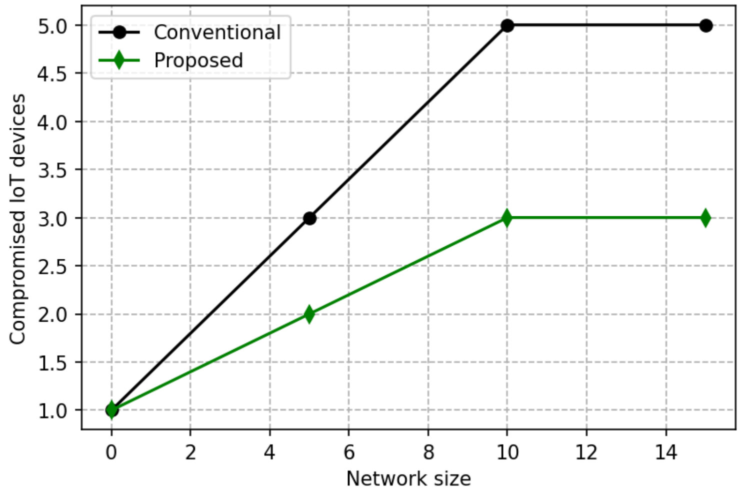


Figure 7: Compromised IoT devices Vs Network size

One potential limitation of the proposed mechanism is that it may require additional computational resources and bandwidth to operate. However, this can be mitigated by optimizing the consensus algorithm and smart contract, and by using a block chain technology that is specifically designed for low-power devices and networks. The proposed mechanism has the potential to significantly enhance the security of IIoT systems, making them more resilient to malware attacks and other security threats. Further research is needed to evaluate the effectiveness and efficiency of the mechanism in real-world settings, and to optimize its performance for different types of IIoT systems and applications.

5. Conclusion:

The proposed mechanism for malware detection in IIoT using block chain technology is a novel approach to improve the security and trustworthiness of IIoT systems. The use of block chain technology provides a decentralized, transparent, and immutable platform for the detection and validation of malware in IIoT networks. The consensus algorithm and smart contract deployed on the blockchain network ensure the integrity of the detection results and provide an additional layer of security and accountability. The results of the proposed mechanism show that it can effectively detect and prevent malware attacks in IIoT networks with minimal overhead of data integrity. The system is also scalable and can be easily integrated with existing IIoT systems without significant modifications. The proposed mechanism has the potential to address the security challenges faced by IIoT networks and enhance the trustworthiness and resilience of these systems. Future research can focus on further improving the performance and efficiency of the system and exploring its applicability in other domains beyond IIoT.

References:

[1] Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, 102481.

[2] Wang, E. K., Liang, Z., Chen, C. M., Kumari, S., & Khan, M. K. (2020). PoRX: A reputation incentive scheme for blockchain consensus of IIoT. Future Generation Computer Systems, 102, 140-151.

[3] Yu, K., Tan, L., Aloqaily, M., Yang, H., & Jararweh, Y. (2021). Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. IEEE transactions on industrial informatics, 17(11), 7669-7678.

[4] H. Moosavi and F. M. Bui, “Delay-aware optimization of physical layer security in multi-hop wireless body area networks,” IEEE Trans. Inf. Forensics Secur., vol. 11, no. 9, pp. 1928–1939, Sep. 2016, doi: 10.1109/TIFS.2016.2566446

[5] 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.

[6] B. Chen, L. Wu, H. Wang, L. Zhou, and D. He, “A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks,” IEEE Trans. Veh. Technol., vol. 69, no. 6, pp. 5813–5825, Jun. 2020.

[7] Liu, M., Yu, F. R., Teng, Y., Leung, V. C., & Song, M. (2019). Performance optimization for blockchain-enabled industrial Internet of Things (IIoT) systems: A deep reinforcement learning approach. IEEE Transactions on Industrial Informatics, 15(6), 3559-3570.

[8] Zelbst, P. J., Green, K. W., Sower, V. E., & Bond, P. L. (2020). The impact of RFID, IIoT, and Blockchain technologies on supply chain transparency. Journal of Manufacturing Technology Management, 31(3), 441-457.

[9] Zhao, S., Li, S., & Yao, Y. (2019). Blockchain enabled industrial Internet of Things technology. IEEE Transactions on Computational Social Systems, 6(6), 1442-1453.

[10] Wen, Q., Gao, Y., Chen, Z., & Wu, D. (2019, May). A blockchain-based data sharing scheme in the supply chain by IIoT. In 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS) (pp. 695-700). IEEE.

[11] Wang, J., Chen, J., Ren, Y., Sharma, P. K., Alfarraj, O., & Tolba, A. (2022). Data security storage mechanism based on blockchain industrial Internet of Things. Computers & Industrial Engineering, 164, 107903.

[12] Wang, Q., Zhu, X., Ni, Y., Gu, L., & Zhu, H. (2020). Blockchain for the IoT and industrial IoT: A review. Internet of Things, 10, 100081.

[13] Seok, B., Park, J., & Park, J. H. (2019). A lightweight hash-based blockchain architecture for industrial IoT. Applied Sciences, 9(18), 3740.

[14] Cao, B., Wang, X., Zhang, W., Song, H., & Lv, Z. (2020). A many-objective optimization model of industrial internet of things based on private blockchain. IEEE Network, 34(5), 78-83.

[15] Rathee, G., Ahmad, F., Jaglan, N., & Konstantinou, C. (2022). A Secure and Trusted Mechanism for Industrial IoT Network using Blockchain. IEEE Transactions on Industrial Informatics, 19(2), 1894-1902.

[16] Suhail, S., Hussain, R., Jurdak, R., & Hong, C. S. (2021). Trustworthy digital twins in the industrial internet of things with blockchain. IEEE Internet Computing, 26(3), 58-67.

[17] Iqbal, S., Noor, R. M., Malik, A. W., & Rahman, A. U. (2021). Blockchain-enabled adaptive-learning-based resource-sharing framework for IIoT environment. IEEE Internet of Things Journal, 8(19), 14746-14755.

[18] Yao, H., Mai, T., Wang, J., Ji, Z., Jiang, C., & Qian, Y. (2019). Resource trading in blockchain-based industrial Internet of Things. IEEE Transactions on Industrial Informatics, 15(6), 3602-3609.

[19] Atlam, H. F., & Wills, G. B. (2019). Technical aspects of blockchain and IoT. In Advances in computers (Vol. 115, pp. 1-39). Elsevier.

[20] Pennino, D., Pizzonia, M., Vitaletti, A., & Zecchini, M. (2022). Blockchain as IoT Economy enabler: A review of architectural aspects. Journal of Sensor and Actuator Networks, 11(2), 20.