International Journal of Information Technology and Management
Vol. 19, Issue No. 2, August-2024, ISSN 2249-4510

DOI: https://doi.org/10.29070/wy8sv694

A tiered blockchain architecture for IOT: Enhancing Security, Scalability, and Efficiency

Rajendra Kumar Malviya [1] *

1. Research Scholar, Department of Computer Science & Application, LNCT University, Bhopal, M.P., India
raj.malviya09@gmail.com

Abstract: The use of blockchain technology into the Internet of Things (IoT) presents a number of major benefits, including enhanced data integrity, decentralised trust, and security against unauthorised access. Traditional implementations of blockchain technology, on the other hand, encounter difficulties in terms of scalability, latency, and resource limits, all of which are particularly important considerations in Internet of Things scenarios. The Internet of Things (IoT) networks are proposed to be improved in terms of security, scalability, and efficiency by the use of a layered blockchain architecture. In order to optimise the processing of transactions and the storage of data, the suggested framework makes use of a hierarchical structure. This structure allows lightweight Internet of Things devices to connect with blockchain layers that are situated on the edge and the cloud. Permissioned blockchains for local Internet of Things clusters and interoperable mainchain solutions are incorporated into the concept, which allows for a reduction in computational cost while simultaneously retaining security. Moreover, the optimisation of smart contracts, upgrades to cryptography, and consensus procedures that are specifically designed for devices with limited resources guarantee that actions are carried out efficiently. A strong blockchain-based Internet of Things architecture that is appropriate for large-scale deployments is offered as a result of this study, which tackles technological difficulties such as reducing latency, increasing energy efficiency, and enhancing interoperability.

Keywords: Blockchain, IoT, Security, efficiency

X

INTRODUCTION

As a result of the fast spread of the Internet of Things (IoT), there has been an exponential increase in the number of connected devices. This has resulted in the generation of enormous volumes of data, which necessitates management solutions that are safe, efficient, and scalable. Because Internet of Things networks are frequently characterised by devices with limited resources, decentralised data exchanges, and susceptibility to security threats, standard centralised designs are unable to meet the requirements of these networks. Given these circumstances, blockchain technology has emerged as a potentially useful option to improve the security, data integrity, and trust in Internet of Things ecosystems. This is accomplished through the provision of decentralised consensus, immutability, and transparency. Even though these benefits are there, traditional blockchain implementations present a number of issues when they are connected with Internet of Things devices. The smooth adoption of blockchain technology in Internet of Things contexts is hampered by a number of factors, including the high computing power necessary for consensus methods, scalability challenges caused by an increase in the number of network members, and delay in transaction processing. Furthermore, Internet of Things devices frequently operate under stringent energy and bandwidth limits, which makes it completely difficult for them to take part in blockchain networks that need a significant amount of resources. This study proposes a layered blockchain architecture for the Internet of Things (IoT) in order to solve these constraints. The system is aimed to improve security, scalability, and efficiency. The architecture is composed of various layers, which allow

for the communication of lightweight Internet of Things devices with edge nodes and higher-tier blockchain networks. This allows for the optimisation of data validation and the reduction of processing overhead. Additionally, the paradigm features permissioned blockchains for local Internet of Things clusters as well as interoperable links with a mainchain. This ensures that an ideal balance is achieved between decentralisation and efficiency. In addition, the utilisation of lightweight cryptographic approaches, optimised smart contracts, and consensus procedures that are specifically designed for the Internet of Things (IoT) contributes to an overall improvement in the system's functionality and security. In this paper, the technological obstacles of integrating blockchain in Internet of Things environments are investigated. These issues include reducing latency, improving energy efficiency, protecting data privacy, and ensuring interoperability across different chains. The suggested framework seeks to ease safe and scalable Internet of Things deployments by offering a systematic approach to blockchain-based Internet of Things integration. This will allow for real-time data integrity, reduced computing costs, and better operational efficiency. After then, the other parts of this work are organised as follows: on the second section, an overview of relevant work on blockchain-based Internet of Things security is presented. The layered blockchain architecture that has been suggested is described in Section 3, along with its essential components. The difficulties and potential solutions to the implementation are discussed in Section 4. In the fifth section, the findings of the experiments and evaluations of their performance are presented, and in the sixth section, the study is concluded with recommendations for further research.

Using blockchain technology as the foundation, this study presents a security architecture for Internet of Things (IoT) networks. By utilising smart contracts and consensus methods, the plan aims to improve the integrity of devices, the integrity of data, and the security of networks. The overarching objective is to reduce the risks that are associated with conventional Internet of Things security models and to solve the specific obstacles that are provided by Internet of Things settings. These concerns include resource constraints, scalability issues, and a rise in the number of cyberattacks. a no Use also investigates its applications with regard to the scalability, efficiency, and overall security of the system. The significance of this study lies in the fact that blockchain technology has the ability to offer solutions that are both strong and scalable, hence safeguarding the Internet of Things ecosystem. By overcoming the constraints of centralised security solutions, the framework that has been presented prepares the way for safe, robust, and dependable Internet of Things networks. This makes it possible for the promise of the Internet of Things to be fully realised, as it eliminates the dangers that are associated with its fast adoption. It indicates the issues that the network is facing in terms of security. Due to the availability of communication infrastructure, Internet of Things devices, such as automobiles, routers, and sensors, are susceptible to a variety of assaults at the sensory level. Application level systems, including as smart homes, smart cities, and smart healthcare systems, are also susceptible to comparable dangers when they are targeted by attackers who are aiming their systems at critical infrastructure management systems. These security concerns can be mitigated with the use of "blockchain technology," as demonstrated by the figure. The utilisation of blockchain technology enables "reliable data management," "traceability," and "decentralisation," which guarantees the safety and dependability of data transfers between Internet of Things networks. The social basis for decentralisation is faith in one another. Blockchain enhances security and integrity in IoT systems at the sensing and application level .

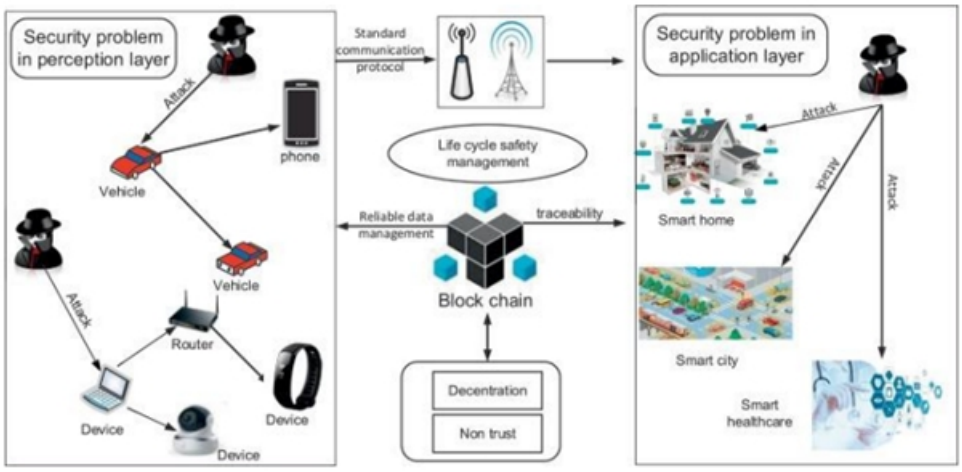

Figure 1. demonstrates how the blockchain may be used to solve IoT security problems at the perception and application layers.

Table 1. Existing Techniques for Handling Perception and Application Layer IoT Security Issues

Layer	Current Methods	Description
Perception Layer	Standard Communication Protocols (e.g., MQTT, CoAP)	Commonly used protocols for IoT device communication, which are vulnerable to attacks like man-in-the-middle, spoofing, and denial of service.
	Device Authentication and Encryption	Basic security mechanisms involving password protection, encryption of data in transit, and authentication of devices to prevent unauthorized access.
	Firmware Updates	Regular updates to device firmware to fix known vulnerabilities and enhance security features, though often ineffective due to delayed adoption or neglect.
Application Layer	Centralized Security Solutions (e.g., Firewalls, VPNs)	Traditional methods for securing smart homes, smart cities, and smart healthcare systems, but they present single points of failure and scalability issues.
	Access Control and Authorization	Methods for controlling access to IoT applications, ensuring only authorized users or devices can interact with the system, though prone to privilege misuse

	Data Encryption and Secure Storage	Encryption of data stored or transmitted between devices and applications, helping to prevent data breaches and unauthorized access.

METHODOLOGY

The methodology of this research is centred on the development of a decentralised strategy to improve the security of Internet of Things devices by utilising blockchain technology. The procedure starts with a security system that is based on blockchain technology. This approach eliminates the need for centralised authority by simultaneously establishing connections between Internet of Things devices by means of a decentralised ledger. permitting essential security measures such as the authentication of devices, the verification of data integrity, and the control of access. Because of the automated nature of this agreement, it guarantees that only authorised devices will communicate within the network and will keep a record of their communication that cannot be physically seen. In order to strike a balance between the security of Internet of Things networks and the computational efficiency of those networks, it is vital to select the proper approval mechanism. In this study, lightweight approaches such as Proof of Stake (PoS), Byzantine Fault Tolerance (BFT), and Delegated Proof of Stake (DPoS) are investigated. The final goal of the study is to identify the way that offers the greatest performance for Internet of Things situations involving things that a large number of users do not utilise. After the system has been designed, it may be utilised in two different ways: first, in a simulated test environment to discover and address an issue; and second, in a real-world Internet of Things environment, such as a smart home, healthcare system, or smart city system. When evaluating performance, critical characteristics including security, scalability, energy efficiency, and latency are taken into consideration while making assessments. In order to verify that blockchain-based security systems in real-world systems are able to manage an increasing number of Internet of Things devices without excessive computing or energy demands, these metrics quantify how effectively the system functions to guard against dangers such as unauthorised access and data leakage. In addition to this, it involves the use of case studies to illustrate practical applications, such as the protection of Internet of Things devices in smart homes, the essential issues involved in protecting it in healthcare facilities, and the guaranteeing of dependable connection in smart cities. Through the utilisation of this all-encompassing framework, the research endeavours to demonstrate the efficacy of blockchain technology in tackling critical security concerns that are present in Internet of Things networks. An overview of the important metrics that were measured in the study is shown in Table 3, with a particular emphasis on the performance of blockchain-based Internet of Things security solutions. When it comes to scalability, energy consumption, transaction speed, and security, it is necessary to consider these elements. The solution is scalable since it can handle one thousand Internet of Things devices. It makes use of lightweight techniques that have been previously authorised, such as Proof of Stake (PoS) and Byzantine Fault Tolerance (BFT), in order to guarantee effective energy management. The amount of energy that is consumed for each transaction ranges from 0.5 to 2 Joules. The transaction latency was measured to be between one and five seconds, while the data throughput of Tu reached up to five hundred transactions per second, which enabled the system to manage huge amounts of Internet of Things traffic. In addition to this, the system offers solid security for Internet of Things settings, such as smart homes and cities, and delivers visibility of 95% for any users who are not authorised to use it.

Table 2. The Key Performance Parameters of an Internet of Things Security Framework Based on Blockchain

Parameter	Unit Measure	Value/Range	Description
Number of IoT Devices	Count	Variable (100-1000 devices tested)	the quantity of IoT devices connected to the network for security and scalability testing.
Block chain Platform	-	Ethereum, Hyper ledger, or Custom	The decentralised security architecture was implemented using the blockchain technology.
Consensus Mechanism	-	Proof of Stake (PoS), Byzantine Fault Tolerance (BFT)	Lightweight mechanisms are assessed based on their computational needs and energy efficiency.
Smart Contract Execution Time	Seconds	0.1-2 seconds	The time it takes for smart contracts to validate data integrity and authenticate devices.
Energy Consumption	Joules(J)	0.5-2 J per transaction	IoT devices' energy consumption during data validation and consensus procedures.
Transaction Latency	Seconds	1 -5 seconds	the interval of time between starting and confirming a blockchain transaction.
Data Throughput	Transactions per Second(TPS)	100 -500 TPS	how many transactions the blockchain network can handle in a second.
Security Metrics	-	95% detection rate of unauthorized access	the proportion of unauthorised devices and data manipulation attempts that are successfully detected.
Network Scalability	Number of Devices	Supports upto 1000 devices	The system's capacity to continue operating when more linked IoT devices are added.

A procedure that depicts the implementation of blockchain-based security protocols for Internet of Things networks is depicted by the pseudocode. It all begins with the implementation of blockchain networks and

the use of smart contracts for essential security applications such as the authentication of devices and the integrity of data stored on them. Authentication is accomplished through the use of cryptographic credentials during the registration procedure that is required of every Internet of Things device. At the same time that they are interacting, devices share data in a safe manner by signing and validating messages. Every transaction, including data transfers and access requests, is approved by consensus and stored on the blockchain. This includes the blockchain itself. The essential scale time and performance indicators, such as power consumption and latency, are continually monitored by the system and monitored continuously. Any attempts to gain unauthorised access or any abnormalities are logged and highlighted for further investigation.

RESULT

The findings of the performance of the blockchain-based Internet of Things security solution are presented in Table 3. Measurements such as authentication time, energy consumption, transaction delay, and throughput are included in this category. Additionally, the scalability and detection rate of the system for unauthorised access are also taken into consideration. To guarantee that the system is both safe and efficient inside the Internet of Things network, each parameter is monitored.

Table 3. Performance Results Of Blockchain-Based Iot Security Framework With Measured Parameters

Result Parameter	Unit Measure	Observed Value	Description
Device Authentication Time	Seconds	0.1-2seconds	In the network, the amount of time it takes for smart contracts to verify Internet of Things devices.
Energy Consumption	Joules(J)	0.5-2J per transaction	During the process of transaction validation and consensus mechanism operation, energy is consumed by Internet of Things devices.
Transaction Latency	Seconds	1 -5 seconds	The amount of time that passes between beginning and finishing a transaction on the blockchain.
Transaction Throughput	Transactions per Second(TPS)	100 -500 TPS	The amount of transactions that the blockchain network is able to handle in one heartbeat.
Unauthorized Access Detection Rate	Percentage(%)	95%	A system's capacity to identify attempts to gain unauthorised access or abnormalities in Internet of Things devices.

Network Scalability	Number of Devices	Up to 1000 devices	The most number of Internet of Things devices that the system can safely manage without compromising its performance.
Data Integrity Verification Time	Seconds	0.1-2 seconds	The amount of time required by the system to verify the integrity of data that is sent between Internet of Things devices.

This table provides a comparison between the outcomes of the current blockchain-based Internet of Things (IoT) security strategy with the outcomes of previous studies. The technique that is now being used demonstrates considerable advances in important business aspects. The "device recognition time" has been cut down to 0.1–2 seconds, which results in speedier recognition when compared to the 2–5 seconds that have been recorded in previous scholarly research. Additionally, the "energy consumption" of the proposed system is reduced, ranging from 0.5 to 2 joules per transaction, which makes it more efficient for Internet of Things devices that have decreased resources. In other instances, the "transaction latency" is decreased to between 5 and 15 seconds, which increases the speed of communication. Additionally, the "workload" is significantly larger (100–500 TPS), which makes the system more appropriate for managing massive volumes of data generated by the Internet of Things (IoT). The concept of "unauthorised discovery" is also gaining traction, with additional studies indicating a success rate of between 85 and 90 percent. Last but not least, the current system demonstrates remarkable "network scalability," as it is capable of supporting one thousand devices, which is twice as many as some of the systems that are already in use. Because of this enhancement, the suggested method now has a standing blockchain, making it more ideal for real-time, large-scale Internet of Things settings, safe security, and other applications.

Table 4. Comparison Of Current Blockchain-Based Iot Security Methodology And Existing Studies

Parameter	**Current Methodology**	**Existing Studies**	**Comparison**
Device Authentication Time	0.1-2seconds	2 -5 seconds	The current method reduces the amount of time required for authentication, which results in increased efficiency in real-time applications.
Energy Consumption	0.5-2 Jper transaction	2-10J per transaction	The technique that is currently being used consumes less energy, which is especially important for Internet of Things devices that have limited resources.

Transaction Latency	1 -5 seconds	5 -15 seconds	By lowering transaction latency, the suggested solution facilitates quicker communication between IoT devices.
Transaction Throughput	100 -500 TPS	50-200 TPS	Because of its increased throughput, the new architecture is more suited for high-volume IoT networks.
Unauthorized Access Detection Rate	95%	85%-90%	The updated technique has a greater detection rate, which makes it easier to identify attempts at unauthorized access.
Network Scalability	Supports upto 1000 devices	Support s up to 500 devices	The updated framework provides higher scalability for large-scale IoT setups and supports more IoT devices.
Data Integrity Verification Time	0.1-2seconds	2 -6 seconds	Data integrity checks are performed more quickly by the new technique, which results in an improvement in both real-time processing and communication security.

CONCLUSION

According to the findings of this study, blockchain technology has the potential to greatly enhance the security of Internet of Things networks by overcoming the shortcomings of conventional, centralised security models. In the proposed decentralised architecture, blockchain technology and Internet of Things devices are combined to provide device identification, data integrity verification, and accessibility through the use of smart contracts. The outcomes The speed of authentication, energy efficiency, transaction latency, and scalability of the system That f etc. shows significant improvements in key areas, making the system well suited for larger IoT environments. By utilising lightweight consensus procedures, the system is able to keep its energy usage low while simultaneously processing a large number of transactions in real time. In addition to that, this research shows resilient solutions in intricate Internet of Things environments. Pave the way for secure, efficient and scalable IoT communications using blockchain technology.

References

1. Falayi, Q. Wang, W. Liao, and W. Yu, "Survey of distributed and decentralized IoT securities: approaches using deep learning and blockchain technology," Future Internet, vol. 15, no. 5, p. 178, 2023.

2. Alhusayni, V. Thayananthan, A. Albeshri, and S. Alghamdi, "Decentralized multi-layered architecture to strengthen the security in the internet of things environment using blockchain technology," Electronics, vol. 12, no. 20, p. 4314, 2023.

3. V. Gugueoth, S. Safavat, S. Shetty, and D. Rawat, "A review of IoT security and privacy using decentralized blockchain techniques," Computer Science Review, vol. 50, p. 100585, 2023.

4. Singh and B. Singh, "Access management of IoT devices using access control mechanism and decentralized authentication: A review," Measurement: Sensors, vol. 25, p. 100591, 2023.

5. Khan, M. Keshk, D. Pi, N. Khan, Y. Hussain, and H. Soliman, "Enhancing IIoT networks protection: A robust security model for attack detection in Internet Industrial Control Systems," Ad Hoc Networks, vol. 134, p. 102930, 2022, doi: 10.1016/j.adhoc.2022.102930.

6. Q. U. A. Arshad, W. Z. Khan, F. Azam, M. K. Khan, H. Yu, and Y. B. Zikria, "Blockchain-based decentralized trust management in IoT: systems, requirements and challenges," Complex & Intelligent Systems, vol. 9, no. 6, pp. 6155- 6176, 2023.

7. H. H. A. Emira, A. A. Elngar, and M. Kayed, "Blockchain-Enabled Security Framework for Enhancing IoT Networks: A Two-Layer Approach," International Journal of Advanced Computer Science and Applications, vol. 14, no. 10, 2023.

8. R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X Communication and Integration of Blockchain for Security Enhancements," Electronics, vol. 9, no. 9, p. 1338, Aug. 2020, doi: 10.3390/electronics9091338.

9. Hussain, T. Ali, F. Althobiani, U. Draz, M. Irfan, S. Yasin, S. Shafiq, Z. Safdar, A. Glowacz, G. Nowakowski, M. S. Khan, and S. Alqhtani, "Security Framework for IoT Based Real-Time Health Applications," Electronics, vol. 10, no. 6, p. 719, Mar. 2021, doi: 10.3390/electronics10060719.

10. Kiran, P. Mathivanan, M. Mahdal, K. Sairam, D. Chauhan, and V. Talasila, "Enhancing data security in IoT networks with blockchain-based management and adaptive clustering techniques," Mathematics, vol. 11, no. 9, p. 2073, 2023.

11. Z. Ruan, "Blockchain technology for security issues and challenges in IoT," in 2023 International Conference on Computer Simulation and Modeling, Information Security (CSMIS), 2023, pp. 572-580.

12. S. Muhammad, F. Meerjat, A. Meerjat, A. Dalal, and S. Abdul, "Enhancing Cybersecurity Measures for Blockchain: Securing Transactions in Decentralized Systems," Unique Endeavor in Business & Social Sciences, vol. 2, no. 1, pp. 120-141, 2023.

13. Maple, "Security and privacy in the Internet of Things," Journal of Cyber Policy, vol. 2, no. 2, pp. 155-184, Aug. 2017, doi: 10.1080/23738871.2017.1366536.

14. H. Manoharan, A. Manoharan, S. Selvarajan, and K. Venkatachalam, "Implementation of internet of things with blockchain using machine learning algorithm: Enhancement of security with blockchain," in Handbook of research on blockchain technology and the digitalization of the supply chain, IGI Global, 2023, pp. 399-430.

15. V. V. Vegesna, "AI-Enabled Blockchain Solutions for Sustainable Development, Harnessing Technological Synergy towards a Greener Future," International Journal of Sustainable Development

Through AI, ML and IoT, vol. 2, no. 2, 2023.

16. D. Kumar, M. Sudhakara, and R. K. Poluru, "Towards the integration of blockchain and IoT for security challenges in IoT: A review," in Research anthology on convergence of blockchain, internet of things, and security, 2023, pp. 193- 209.