A Review on Blockchain based secure communication for IoT Devices

Mrs. Minal S. Darekar
PhD. Scholar, School of Information Technology, Indira University, Pune. Assistant Professor, Department of Computer Science, IT & Animation, Deogiri College, Chh. Sambhajinagar-431005.

Dr. Madhavi Avhankar
Assoc. Professor, School of Information Technology, Indira University, Pune.

DOI: 10.29322/IJSRP.16.02.2026.p17022
https://dx.doi.org/10.29322/IJSRP.16.02.2026.p17022

Paper Received Date: 9th January 2026
Paper Acceptance Date: 8th February 2026
Paper Publication Date: 12th February 2026

Abstract

The Internet of Things (IoT) connects a massive number of heterogeneous devices that exchange sensitive data over open networks, making security, trust, and privacy critical challenges. Conventional centralized security models suffer from single points of failure, limited scalability, and vulnerability to cyberattacks such as data tampering, spoofing, and unauthorized access. To address these limitations, this review paper presents a comprehensive analysis of blockchain-based secure communication approaches for IoT systems. It systematically examines existing architectures, consensus mechanisms, authentication schemes, access control models, and data integrity solutions proposed in recent literature. The study categorizes blockchain-IoT integration techniques based on network type, security objectives, and performance constraints, with particular emphasis on lightweight and energy-efficient solutions suitable for resource-constrained IoT devices. Furthermore, the paper highlights key challenges such as scalability, latency, interoperability, storage overhead, and privacy concerns. By identifying research gaps and open issues, this review provides valuable insights into future research directions and design considerations for developing scalable, secure, and efficient blockchain-enabled IoT communication frameworks. The findings serve as a useful reference for researchers and practitioners aiming to enhance trust and security in next-generation IoT systems.

Index Terms- Blockchain, Centralized, Decentralized, Devices, Internet of Things (IoT), Protocols, Privacy, Security, Scalability, Threats.

I. INTRODUCTION

The significance of the Internet of Things (IoT) in the development of smart applications is increasing in recent times [1]. The IoT echo system is heterogeneous and dynamic with multiple devices and protocols. IoT adoption is widespread with many challenges regarding resources, deployment, architecture, security, and protocols for achieving Service of Security [2]. IoT transforms the conventional applications into smart applications by incorporating advanced and sophisticated technologies and thereby helps in improving the productivity and quality of the service. Due to the increased adoption of IoT, more data is being generated in the systems [2]. With the increase in the adaptability of IoT systems, the concerns related to the security and privacy of IoT data is also increasing [1].

Due to the limited processing capabilities of IoT devices, IoT devices usually leverage externally controlled third party service providers to perform additional data processing. By transmitting sensitive user data to third party services providers, users are forced to trust service providers to enforce data protection and provide data privacy guarantee. Unfortunately, service providers often violate data privacy policies by using data collected from users for unauthorized purposes. This undue advantage by service providers is based on centralized architecture where trust in a third party system as a central authority is required to manage user data [3]. A centralized approach is susceptible to a wide range of security and privacy problems, including single points of failure, false data injection, Sybil vulnerabilities, issues of trust between participants, and difficulties with file accessibility and Retrieval [4]. In order to eliminate these imbalance in data access policy enforcement between service providers and users, we propose a system of decentralized data management using decentralized asset management system based on Blockchain and smart contract technology [5].

Blockchain, as a decentralized and distributed technology, offers potential solutions. With blockchain's capability to provide decentralized trustworthy storage, the access control policies and records in a distributed system can be securely stored on the blockchain without tampering, and the system is also equipped with strong auditability. Furthermore, the emergence of smart contracts expands the ability of blockchain for various decentralized applications. Thus, blockchain can act as a secure and trustworthy decentralized platform, providing strong traceability and verifiability for IoT access control [6].

1.1 BLOCKCHAIN TECHNOLOGY

Blockchain technology provides new ways of designing a decentralized system architecture. Blockchain is intended to improve security and trust between users where the transaction data can be shared across an unsecured network of participants without the mediation of centralized third parties. Blockchain was originally developed by Satoshi Nakamoto in 2008 as a peer-to-peer money exchange technique via a digital cryptocurrency known as Bitcoin [13]. The term "Blockchain" originated from its technical structure (Chain Blocks), meaning the association of each block with the block that precedes it [14]. Blockchain provides a decentralized platform for IoT applications which avoids the chances of a single point of failure. In general, Blockchain technology is defiant to data modification. In other words, the changes made in one of the ledgers are distributed to all the nodes participating in the transaction and the modified data is updated in the ledger. Once the transaction is authenticated from all the nodes in the network, it is impossible to modify the transaction without modifying the data in the previous blocks [1].

In general, Blockchain is categorized into three types namely public, private, and hybrid or consortium Blockchain. They are categorized based on their ability to give permission to the users for interacting with the Blockchain network [1, 4].

Table1: Comparison amongst public, consortium and private blockchains [17].

Feature	Public Blockchain	Private Blockchain	Consortium Blockchain
Decentralization	Fully decentralized, open to all participants	Partially decentralized, controlled by a single entity	Semi-decentralized, governed by multiple organizations
Security	High (due to consensus mechanisms like PoW/PoS)	Medium (depends on internal security policies)	High (collaborative security policies)
Scalability	Low (due to high computational and storage requirements)	High (optimized for speed and efficiency)	Medium (scalable but requires multi-party coordination)
Transaction Speed	Slow (minutes to hours, depends on network congestion)	Fast (near-instant transactions)	Moderate (depends on the number of validators)
Energy Efficiency	Low (PoW requires high energy consumption)	High (less computationally intensive)	Moderate (depends on consensus mechanism)
Access Control	Open to all users	Restricted to authorized participants	Restricted to selected organizations
Best Suited For	Decentralized applications, cryptocurrencies, public data verification	Enterprise applications, supply chain, healthcare, financial services	Industrial IoT, smart grids, inter-organizational collaboration
Examples	Bitcoin, Ethereum	Hyperledger Fabric, Corda	IBM Blockchain, R3 Corda Consortium

Consensus algorithms are an integral part of the Blockchain technology which are responsible for maintaining the integrity, confidentiality, and security of the Blockchain platform. Consensus algorithms are different for different Blockchain. The most prominent consensus algorithms are Proof of Work (POW), Proof of stake (PoS), Byzantine fault-tolerant (BFT), Proof of Authority (PoA), Proof of Elapsed Time (PoET) [1].

Here's a comprehensive comparison of different blockchain consensus algorithms in the context of secure communications for IoT devices — focusing on security, resource efficiency, scalability, and suitability for resource-constrained environments like IoT:

Table2:

Consensus Algorithm	Security	Resource Efficiency	Scalability	Suitability
Proof of Work (POW)	High	Very high	Poor	✗ Poor
Proof of stake (PoS)	Strong	Much lighter than PoW	Moderate	✔ Good
Byzantine fault-tolerant (BFT)	Strong	Lower than PoW	High	✔ Excellent
Proof of Authority (PoA)	Strong	Low	High	✔ Good

Proof of Elapsed Time (PoET)	Strong	Low	High	✔ Good

1.2 INTERNET OF THINGS

A typical IoT architecture comprises of devices, sensors, actuators, IoT Hubs, IoT Gateway and a cloud service provider. IoT devices are devices with capability to sense and collect data which can be transmitted on a connected network for storage or further processing. IoT devices includes light bulbs, heart rate monitors, smart cameras and many more. With the IoT hub, different devices with disparate communication protocol such zigbee or bluetooth can connect to the IoT network [3].

1.3 RESEARCH GAP AND MOTIVATION

Although several studies have explored the integration of blockchain for securing IoT communications, the existing literature remains fragmented and largely application-specific. Most prior reviews focus either on general blockchain architectures or isolated IoT security challenges without systematically analyzing secure communication mechanisms such as authentication, access control, data integrity, and privacy in blockchain-enabled IoT environments. Furthermore, current surveys often overlook critical challenges related to scalability, latency, resource constraints of IoT devices, and interoperability across heterogeneous blockchain platforms. As a result, there is a lack of a comprehensive and structured review that categorizes blockchain-based secure communication approaches in IoT, compares their security properties, and identifies open research challenges. To address the identified research gaps, this paper makes the following contributions:

- Presents a comprehensive taxonomy of blockchain-based secure communication mechanisms in IoT, categorizing existing solutions based on communication layers, blockchain type, and security objectives.
- Provides a comparative analysis of state-of-the-art approaches in terms of security properties, consensus mechanisms, scalability, resource efficiency, and suitability for resource-constrained IoT devices.
- Highlights key challenges and limitations, including energy consumption, transaction overhead, privacy leakage, and interoperability issues in blockchain-enabled IoT communication.
- Identifies open research issues and future directions to guide researchers toward developing efficient and secure blockchain-based IoT communication systems.

II. LITERATURE REVIEW

Different types of IoT gadgets generate different kinds of data, like motion detection, temperature, humidity, and face detection. A separate database must store this data. A centralized database system connects all these gadgets and databases. Any user can access any type of data through the centralized database. As the number of users increases, the load on CDB will also increase. The main disadvantage of this type of network is the single point of failure. If CDB is down or having some serious issues, then it will affect the whole network. To solve this problem, we can put multiple copies of CDB so that if one server is facing some issue, a request can be sent to another server. However, if a hacker manages to compromise the CBS and steals confidential files from CDB, it could potentially harm the entire network. So, to solve the security issue of an IoT system, we want to integrate the blockchain with an IoT system. Due to the unique features of private blockchain, it will provide a strong, secure, decentralized, and scalable IoT system; without permission, no one can enter the network [7].

In the paper [7], author proposed an IoT system that utilizes blockchain and Attribute based access control i.e. ABAC policies to enhance both its safety and scalability. To meet the IoT security requirements using a private blockchain, we developed a lightweight and robust access control system. In their proposed architecture, RabbitMQ (AMQP) is used specifically for handling blockchain operations like managing write and retrieval processes, not for direct IoT communication. RabbitMQ was chosen because it offers reliable message delivery, transaction support, and message persistence, which are crucial for scaling blockchain operation features that MQTT lacks. Additionally, RabbitMQ's security aligns with the blockchain's security model. If necessary, we can integrate an MQTT-to-RabbitMQ bridge to connect IoT devices and maintain robust blockchain handling.

In the paper [8], author has proposed various cloud computing access methods for IOT Devices. Access control is an essential element of a security strategy, which regulates the permissions for individuals to access specific resources within a system. Cloud settings provide problems to standard access control approaches due to issues such as centralization, single points of failure, and susceptibility to illegal access. These difficulties need a reassessment of current access control frameworks, leading to the investigation of novel solutions like blockchain. Access control models provide the techniques and regulations employed to oversee and limit access to information or resources, There are five well-known models of cloud computing access control: 1. Role-based access control (RBAC): This streamlines access management by allocating permissions to roles designated by an organization rather than individuals 2. Attribute-based access control (ABAC): This involves the use of user attributes, resources, and environment to determine access. Such attributes can include user roles, time of access, location, and other contextual data that might be useful. 3.

Mandatory access control (MAC): This kind of access control technique is mostly applicable in environments that require extra security, for instance, military and government networks. The MAC systems constrain access decisions through a central authority. 4. Discretionary access control (DAC): Resource owners decide who may access content under discretionary access control. 5. Rule-based access control (ReBAC): This also known as Relationship-Based Access Control, determines access decisions based on the relationships between users and resources

In the paper [9], author has proposed Blockchain-Based Mitigation of De-authentication Attacks (BBMDA) Framework. The BBMDA framework leverages the unique features of blockchain technology, integrates the elliptic curve digital signature algorithm (ECDSA) for authentication, and employs a multitask transformer (MTT) for traffic classification to effectively mitigate de-authentication attacks in IoT environments. By integrating ECDSA for authentication and MTT for traffic classification, the BBMDA framework ensures robust defence against de-authentication attacks in IoT environments. The use of blockchain technology further enhances security, data integrity, and trustworthiness, making IoT ecosystems more resilient to evolving threats. The proposed BBMDA framework paves the way for future research and advancements in IoT security and blockchain applications, promoting a safer and more reliable IoT landscape.

In the paper [10], author has explored about the concept of cyber deception, its key components, and its application in BIoT systems. Cyber deception is a proactive defense mechanism employed to obscure and constantly modify the attack surface. Its primary objective is to mislead attackers, effectively hiding critical assets and leading adversaries to expend resources on fruitless endeavors. This approach delays and exposes attacker behaviour and provides valuable threat intelligence. Key components of cyber deception include honeypots and Moving Target Defense (MTD). Honeypots focus on deploying decoy systems to entrap attackers, while MTD strategies involve the dynamic alteration of the attack surface. Together, these proactive defense methods significantly bolster the security of BIoT systems, creating a more resilient and challenging environment for potential cyber threats.

In the paper [11], author proposed novel lightweight fuzzy extractor and blockchain based secured IoT system that provides data security in two ways. Our system consists of a novel Light weight Time-based Identification Protocol for small IoT devices. Data security is also provided by employing blockchain application in the system for easy data sharing and auditing. Author also presented their implementation work of LiTBIP on the Raspberry Pi platform to evaluate the effectiveness of protocol for a large number of hubs. The scalability analysis of the protocol showed that the computation overhead is very small and constant which makes it an excellent choice for large scale IoT systems.

In the paper [13], author addressed security and efficiency issues in current traditional centralized authentication systems. To this end, they propose an energy-efficient secure architecture that provides lightweight authentication, identity verification, and end-to-end protection of students' learning records in educational environments. This approach would help students to transfer their learning records from one institution to another in a secure and authenticated manner. The security model is based on blockchain technology and can be integrated into IoT-based learning systems with limited computations, lower energy, and minimum memory requirements to provide real-time protection of the collected data. Thus, in this work, an innovative decentralized blockchain-based authentication model is implemented for e-learning and educational environments. The model effectively solves the existing problems and provides a reliable and energy-efficient mechanism to protect the IoT-based e-learning users.

Table3: Comparative Analysis for Literature

References	Year	Proposed Methodology	Contribution	Limitations
[7]	2025	Blockchain and Attribute based access control.	RabbitMQ (AMQP) is used specifically for handling blockchain operations like managing write and retrieval processes.	Direct IoT communication not possible.
[8]	2024	Cloud computing access control methods for IOT Devices.(RBAC, ABAC, MAC, DAC, ReBAC)	Access control models provide the techniques and regulations employed to oversee and limit access to information or resources	Scalability, High Processing cost, Latency, Privacy, Interoperability
[9]	2024	Blockchain-Based Mitigation of De-authentication Attacks (BBMDA) Framework.	By integrating ECDSA for authentication and MTT for traffic classification, the BBMDA framework ensures robust defence against de authentication attacks in IoT	Scalability Enhancements Privacy Considerations real-time deployment optimizations, and exploration of hybrid approaches.

			environments	
[10]	2024	Cyber deception with honeypots and Moving Target Defense (MTD)	This approach delays and exposes attacker behavior and provides valuable threat intelligence.	Improving cost modeling and scaling strategies, addressing data scarcity, reducing computationa overhead, and refining the integration of BIoT components.
[11]	2022	Novel Light weight Time based Identification Protocol for small IoT devices (LiTBIP).	The scalability analysis of the protocol showed that the computation overhead is very small and constant which makes it an excellent choice for large scale IoT systems.	Suitable for small IoT Devices.
[13]	2023	Energy-efficient secure architecture that provides lightweight authentication, identity verification, and end to-end protection of student's learning records in educational environments.	An innovative Decentralized blockchain-based authentication model is implemented for e learning and educational environments.	e-learning data can only be shared by affiliated universities in the network, and the user cannot share learning data directly with another user

III. PERFORMANCE, SCALABILITY AND OVERHEAD CHALLENGES

3.1 PERFORMANCE

In the context of blockchain-based secure communication for IoT Devices, performance is commonly evaluated using metrics such as transaction latency, throughput, communication overhead, computational cost, energy consumption, storage overhead, and scalability with respect to the number of devices and transactions. These metrics are particularly critical due to the resource constraints of IoT devices and the real-time communication requirements of many IoT applications.

3.2 SCALABILITY

Scalability remains a major challenge in blockchain-enabled IoT communication systems. Public blockchains, such as those based on Proof-of-Work (PoW), suffer from limited transaction throughput and high confirmation latency, making them unsuitable for large-scale IoT deployments. Several studies report that as the number of IoT devices increases, transaction congestion and block propagation delays significantly degrade system performance. Although permissioned blockchains and lightweight consensus mechanisms improve scalability, they often introduce trade-offs in decentralization and fault tolerance. Moreover, most existing solutions are evaluated under small-scale testbeds, leaving their scalability under real-world IoT-scale deployments insufficiently explored.

3.3 OVERHEAD

Blockchain integration introduces significant communication and computational overhead in IoT systems. Secure communication protocols built on blockchain typically require additional message exchanges for transaction validation, block confirmation, and smart contract execution. These operations increase bandwidth usage and latency, which is problematic for low-power and low-bandwidth IoT devices. Furthermore, cryptographic operations such as digital signatures and hashing impose computational overhead that may exceed the processing capabilities of constrained devices. Ledger replication also results in substantial storage overhead, particularly in long-running IoT applications where the blockchain continuously grows.

IV. METHODOLOGY

In This study we have used a preliminary literature review methodology to examine the current state of research on blockchain based secure communication for IoT devices, focusing on their security aspects. A preliminary literature review aims to provide an overview of a topic, identify key concepts, and highlight potential areas for future research [10]. This approach is beneficial when addressing emerging or complex topics, such as integrating blockchain and IoT technologies. The preliminary literature review process involves the following steps:

We conducted a broad search for academic articles, conference papers, and book chapters related to IoT, blockchain, and implications for their secure communication. The search used scholarly databases, including IEEE Xplore, ACM Digital Library, Springer Link, Elsevier, MDPI , Wiley Online Library and Google Scholar.

The identified literature was read and analyzed to understand the key concepts, challenges, and opportunities related to blockchain-based IoT systems and their security. We focused on identifying the field's most relevant and influential works during this process.

Based on the literature, we identified gaps in the current research and proposed potential future research directions to address these gaps. This step involved critically analyzing existing approaches' limitations and identifying promising avenues for further exploration.

By following this preliminary literature review methodology, we aim to provide a comprehensive overview of the current state of blockchain-based secure communication in IoT Devices research, identify key challenges and opportunities, and propose a conceptual framework for security optimization in this context. While this approach may not be as systematic as a structured literature review, it allows for a more flexible and open-ended exploration of an emerging and complex topic, enabling us to identify potential areas for future research and innovation.

V. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

This section discusses open challenges and future research directions relevant to Blockchain–IoT integration. Despite the presence of many survey studies in the literature, important research gaps still require further investigation. For the literature paper [7], the work proposed for the integration of Blockchain and IoT addresses many of the vulnerabilities and limitations inherent in traditional IoT control of access systems, setting a new standard for secure and efficient access management. Despite the promising results, future work could further improve the system. Future studies should focus on scaling solutions, such as layer-2 protocols or alternative consensus techniques, exploring standards and frameworks to ensure interoperability between different IoT gadgets, blockchain platforms, message queuing systems, and more energy-efficient consensus algorithms and techniques to reduce the environmental impact of the system. In paper [8] author addressed the primary challenges like scalability of blockchain networks, as the increasing volume of transactions can result in high processing costs and latency, as well as access control privacy problems. Which in turn affects the efficacy of access control systems. Blockchain integration with cloud infrastructures also causes compatibility and interoperability concerns. Future research should develop more scalable and efficient consensus algorithms, explore hybrid blockchain systems with public and private aspects, and improve cryptographic methods to protect sensitive data. These directions aim to improve blockchain access control technology for modern cloud environments. The paper [9] proposed Blockchain-Based Mitigation of Deauthentication Attacks (BBMDA) Framework presents a robust and efficient solution for enhancing the security and trustworthiness of IoT environments. The proposed framework opens avenues for future research, including scalability enhancements, privacy considerations, real-time deployment optimizations, and exploration of hybrid approaches. In the review of paper [10] we have identified several research gaps and open questions that provide a roadmap for future work. These include refining game-theoretic models for BIoT security, enhancing consensus algorithms, developing robust hardware-based security solutions, leveraging AI and machine learning to counteract sophisticated cyberattacks, integrating post-quantum cryptography, and effectively employing zero-knowledge proofs and cyber deception techniques within the BIoT framework. Future research addressing these gaps will involve exploring non-rational attacker behavior, improving cost modeling and scaling strategies, addressing data scarcity, reducing computational overhead, and refining the integration of BIoT components. Our future work includes developing a detailed framework, implementing it in a case study, and evaluating its practicality and effectiveness. In the paper [11] auhor proposed a novel lightweight fuzzy extractor and blockchain based secured IoT system that provides data security in two ways. System consists of a novel Light weight Time-based Identification Protocol for small IoT devices. Large scale real world deployment may introduce new challenges,
such as data integration and configuration issues, that will need to look into.

VI. RESULTS

It is clear from the studied literature that, The blockchain based IoT frameworks provide stronger data integrity and authentication compared to traditional centralized security models. Decentralized ledger architectures significantly enhance trust management in large-scale IoT environments. While blockchain enhances security, privacy preservation remains a challenge, particularly in public blockchain-based IoT systems. Blockchain integration introduces computational and communication overhead, making lightweight consensus mechanisms essential for IoT deployment. Lightweight consensus and edge-assisted architectures significantly improve feasibility for resource-constrained IoT devices. Current blockchain-IoT integration struggle to

scale efficiently in real-time, large-scale environments. The literature review reveals that the scalability, privacy preservation and energy efficiency remain open research challenges.

VII. CONCLUSION

This literature review examined recent research on blockchain-based secure communication frameworks for IoT devices. The analysis indicates that blockchain technology significantly enhances key security requirements such as data integrity, authentication, access control, and trust management by eliminating centralized control and enabling immutable transaction records. Decentralized architectures reduce vulnerability to common cyber-attacks, including data tampering and single-point-of-failure threats, making blockchain a promising solution for securing IoT ecosystems .However, the review also reveals several critical challenges that limit the practical deployment of blockchain in resource-constrained IoT environments. High computational overhead, increased latency, energy consumption, and scalability issues remain major concerns, particularly when traditional consensus mechanisms are used. Although lightweight consensus algorithms, edge-assisted blockchain models, and hybrid architectures show potential in addressing these limitations, they are still in early stages of development and lack large-scale real-world validation. Overall, blockchain-based secure communication offers a robust conceptual foundation for improving IoT security; however, further research is required to bridge the gap between theoretical models and practical, scalable deployments in real-world IoT systems.

REFERENCES

1. Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. (2023). A review of IoT security and privacy using decentralized blockchain techniques. Computer Science Review, 50, 100585.
2. Sivakumar Nagarajan, “A review of IoT security and privacy using the Blockchain to Boost Data Integrity and Privacy”, International Journal of Scientific Research in Engineering & Technology, Volume4, Issue1 (January-February 2024), PP: 59-61
3. Ayoade, G., Karande, V., Khan, L., & Hamlen, K. (2018, July). Decentralized IoT data management using blockchain and trusted execution environment. In 2018 IEEE international conference on information reuse and integration (IRI) (pp. 15-22). IEEE.
4. Al-Barazanchi, I., Murthy, A., Al Rababah, A. A. Q., Khader, G., Abdulshaheed, H. R., Daghighi, E., & Niu, Y. (2022). Blockchain-technology-based solutions for IoT security. Iraqi Journal for Computer Science and Mathematics, 3(1), 6.
5. Ullah, Z., Husnain, G., Mohmand, M. I., Qadir, M., Alzahrani, K. J., Ghadi, Y. Y., & Alkahtani, H. K. (2024). Blockchain-IoT: A revolutionary model for secure data storage and fine-grained access control in internet of things. IET Communications, 18(19), 1524-1540.
6. Jiang, W., Li, E., Zhou, W., Yang, Y., & Luo, T. (2023). IoT access control model based on blockchain and trusted execution environment. Processes, 11(3), 723.
7. Karankar, N., & Seth, A. (2025). An IoT system for access control using blockchain and message queuing system. EURASIP Journal on Information Security, 2025(1), 31.
8. Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024). A systematic review on blockchain-based access control systems in cloud environment. Journal of Cloud Computing, 13(1), 146.
9. Gopalan, S. H., Manikandan, A., Dharani, N. P., & Sujatha, G. (2024). Enhancing IoT security: a blockchain-based mitigation framework for deauthentication attacks. International Journal of Networked and Distributed Computing, 12(2), 237-249.
10. Commey, D., Mai, B., Hounsinou, S. G., & Crosby, G. V. (2024). Securing blockchain-based IoT systems: A review. IEEE Access.
11. Sabrina, F., Li, N., & Sohail, S. (2022). A blockchain based secure IoT system using device identity management. Sensors, 22(19), 7535.
12. Almarri, S., & Aljughaiman, A. (2024). Blockchain technology for IoT security and trust: a comprehensive SLR. Sustainability, 16(23), 10177.
13. Khashan, O. A., Alamri, S., Alomoush, W., Alsmadi, M. K., Atawneh, S., & Mir, U. (2023). Blockchain-Based Decentralized Authentication Model for IoT-Based E-Learning and Educational Environments. Computers, Materials & Continua, 75(2).
14. Alamri, M., Jhanjhi, N. Z., & Humayun, M. (2019). Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review. Int. J. Comput. Sci. Netw. Secur, 19(1), 244-258..
15. Picone, M., Cirani, S., & Veltri, L. (2021). Blockchain security and privacy for the Internet of Things. Sensors, 21(3), 892.
16. Song, H., Tu, Z., & Qin, Y. (2022). Blockchain-based access control and behavior regulation system for IoT. Sensors, 22(21), 8339.
17. Ashalatha P. R. (2019). Blockchain-based secure communication in IoT networks. World Journal of Advanced Research and Reviews, 3(3), 98-107.
18. Kumar, A., Sharma, B., & Noonia, A. (2025). Secure blockchain based intrusion detection for IoT networks. Discover

Computing, 28(1), 226.
19. Arora, D. S. (2025). Secure blockchain-based internet of things (IoT) device management using mixed methods. International journal of scientific and research publications, 14, 12.