Indonesian Journal of Modern Science and Technology Modern (IJMST)
Vol. 1, No. 3, September 2025, pp. 115-124
E-ISSN: 3090-3831 | DOI: doi.org/10.64021/ijmst.1.3.115-124.2025

Blockchain-based Decentralized Authentication and Authorization for IoT Applications

Hewa Majeed Zangana [1,*], Hakem Beitollahi [2], Sabat Salih Muhamad [3], Marwan Omar [4], Firas Mahmood Mustafa [5], Aquil Mirza Mohammed [6], Sharyar Wani [6], Shuai Li [7]
[1] Duhok Polytechnic University, Duhok, Iraq
[2] Soran University, Soran, 44008, Kurdistan, Iraq
[3] Soran University, Soran, 44008, Kurdistan, Iraq
[4] Illinois Institute of Technology, USA
[5] Chemical Engineering Dept., Technical College of Engineering, Duhok Polytechnic University, Duhok, Iraq
[6] The Hong Kong Polytechnic University (PolyU), Hong Kong
[7] Department of Computer Science, IIUM, Kuala Lumpur, Malaysia
[8] University of Oulu, Finland

ARTICLE INFO

Article history:

Received June 23, 2025
Revised September 2, 2025
Published September 30, 2025

Keywords:

Authentication; Blockchain; Cybersecurity; IoT; Scalability;

ABSTRACT (10 PT)

The rapid proliferation of Internet of Things (IoT) devices has introduced significant challenges in ensuring secure and efficient authentication and authorization mechanisms. Traditional centralized approaches are increasingly inadequate due to their single points of failure, scalability issues, and vulnerability to attacks. This paper explores a blockchain-based decentralized framework for authentication and authorization in IoT applications, leveraging the inherent security features of blockchain technology. The proposed solution employs smart contracts to automate and enforce access control policies, ensuring that IoT devices can securely interact without relying on a trusted third party. By integrating blockchain with IoT, this approach enhances data integrity, transparency, and auditability while mitigating common security risks associated with centralized systems. The paper provides a comprehensive analysis of the architecture, implementation details, and performance evaluation, demonstrating the feasibility and advantages of the proposed decentralized authentication and authorization scheme. Experimental results indicate improved security, scalability, and operational efficiency, positioning blockchain as a promising solution for secure IoT environments.

Corresponding Author:

Hewa Majeed Zangana, Duhok Polytechnic University, Duhok, Iraq
Email: hewa.zangana1987@gmail.com

1. INTRODUCTION

The Internet of Things (IoT) represents a paradigm shift in technology, interconnecting a myriad of devices, sensors, and systems, thereby enabling unprecedented levels of automation and data exchange. However, this connectivity comes with substantial cybersecurity risks, making secure authentication and authorization mechanisms crucial. Traditional centralized security models often fail to meet the unique

demands of IoT environments due to scalability issues, single points of failure, and vulnerability to various cyber threats [1].

Blockchain technology, with its decentralized nature, immutability, and cryptographic security, offers a promising alternative to conventional security approaches. By leveraging blockchain, IoT applications can achieve enhanced security, transparency, and resilience against attacks[2]. Blockchain's decentralized ledger eliminates the need for a central authority, distributing trust across the network and ensuring that data cannot be altered once recorded [3], [4].

Smart contracts, a key feature of blockchain, further bolster security by automating and enforcing rules and policies without human intervention. These self-executing contracts can manage access control in IoT systems, ensuring that only authorized devices and users can interact with the network [5]. This approach mitigates many of the risks associated with traditional systems, such as insider threats and unauthorized access [6], [7].

Despite the potential benefits, the integration of blockchain with IoT is not without challenges. Issues such as scalability, latency, and the computational demands of blockchain protocols must be addressed to ensure seamless operation in IoT environments [8]. Additionally, the specific needs of IoT applications, including low power consumption and limited processing capabilities, require tailored blockchain solutions [9], [10].

This paper aims to explore a blockchain-based decentralized framework for authentication and authorization in IoT applications. We will discuss the architecture of the proposed system, its implementation, and the security benefits it offers. Our analysis includes a comprehensive review of existing blockchain and IoT security literature, identifying current challenges and potential solutions [11], [12]. By presenting experimental results and performance evaluations, we demonstrate the feasibility and advantages of using blockchain to secure IoT networks [13], [14].

Although several blockchain-based authentication and authorization schemes for IoT have been reported in the literature, most existing approaches either rely on partially centralized gateways, do not tightly integrate access control with blockchain logic, or fail to address scalability and device-level autonomy simultaneously. Many prior solutions use blockchain mainly as a secure logging mechanism rather than as an active enforcement layer for security decisions.

The novelty of the proposed framework lies in its fully decentralized enforcement of both authentication and authorization through smart contracts, where security decisions are executed directly on the blockchain without dependence on centralized identity servers or external authorization services. Unlike traditional blockchain-based IoT security models that merely store credentials or access records, the proposed approach embeds dynamic access control logic inside smart contracts, enabling real-time validation, revocation, and permission updates for IoT devices.

Furthermore, the proposed architecture is designed specifically for resource-constrained IoT environments, allowing devices to authenticate and obtain permissions through lightweight blockchain interactions rather than heavyweight cryptographic exchanges or centralized brokers. This combination of on-chain access control, decentralized trust management, and IoT-aware design distinguishes the proposed framework from existing blockchain-based IoT security solutions.

The main contributions of this study are summarized as follows:

- A fully decentralized blockchain-based authentication and authorization framework for IoT systems that eliminates reliance on centralized identity providers and access control servers.
- A smart contract–driven access control model that enforces authentication, authorization, and permission management directly on the blockchain, ensuring tamper-proof and transparent security decisions.
- An integrated system architecture that connects IoT devices with blockchain nodes in a secure and scalable manner, supporting secure device-to-device and device-to-service communication.
- A comprehensive experimental evaluation that analyzes security, scalability, latency, and energy efficiency of the proposed framework in a realistic IoT environment.
- A comparative assessment showing the advantages of the proposed decentralized approach over traditional centralized IoT security solutions in terms of security, trust, and fault tolerance.

The following sections provide an in-depth examination of blockchain technology's role in enhancing IoT security, addressing key cybersecurity concerns, and outlining future research directions to further refine and optimize this integration [15], [16].

2. LITERATURE REVIEW

The increasing interconnectivity of IoT devices poses significant cybersecurity challenges, necessitating robust authentication and authorization mechanisms. Blockchain technology has emerged as a potential solution to enhance the security of IoT systems, given its decentralized nature, immutability, and cryptographic principles. This section reviews existing literature on the application of blockchain in enhancing cybersecurity, focusing on IoT environments.

Recent research has increasingly focused on blockchain-based authentication and authorization mechanisms specifically designed for IoT environments. These studies highlight how decentralized identity management and smart-contract-based access control can overcome the limitations of traditional centralized IoT security models. Existing work emphasizes the importance of scalable, low-latency, and energy-efficient authentication frameworks tailored to resource-constrained IoT devices, thereby reinforcing the relevance of blockchain-driven access control in IoT-centric security architectures.

Blockchain's decentralized trust model is crucial in IoT environments, where central authorities often become points of failure. Discuss how blockchain technologies provide security against cyberattacks, highlighting the elimination of centralized vulnerabilities [17]. Similarly, elaborates on blockchain's applications, emphasizing its role in enhancing data integrity and transparency in IoT networks [5].

Smart contracts, a fundamental feature of blockchain, automate and enforce access control policies without human intervention. These contracts ensure that only authorized entities interact with IoT devices, thereby reducing the risk of unauthorized access. Explore the implications of blockchain and smart contracts for cybersecurity, particularly in automating security protocols and reducing human error [16][2].

Despite its benefits, blockchain technology faces challenges related to scalability and performance, which are critical in IoT applications. Survey blockchain cybersecurity vulnerabilities and possible countermeasures, highlighting the need for scalable solutions to handle the high volume of transactions in IoT networks [8]. Provide a systematic literature review on blockchain for cybersecurity in the food supply chain, pointing out the importance of efficient consensus mechanisms to maintain performance [18].

Integrating blockchain with IoT requires addressing specific needs such as low power consumption and limited processing capabilities of IoT devices. Examine the integration of blockchain and AI for next-generation energy grids, discussing cybersecurity challenges and opportunities [10]. Similarly, discuss blockchain opportunities and issues in the built environment, focusing on trust, transparency, and cybersecurity [9].

Practical applications and case studies demonstrate blockchain's effectiveness in enhancing IoT security. Present a case study on the impacts and potential of blockchain technology in enhancing the security and reliability of information systems [7]. Investigate blockchain's impact on European banks' cybersecurity and data integrity, illustrating the technology's practical benefits in financial sectors [4].

Future research should focus on developing tailored blockchain solutions that meet the unique demands of IoT applications. Conduct a scoping review on the cybersecurity challenges in blockchain technology, suggesting avenues for future research [11]. Provide comprehensive reviews of blockchain's role in contemporary business cybersecurity, emphasizing the need for innovative solutions to emerging threats [12][19].

The literature indicates that blockchain technology offers significant potential to enhance IoT cybersecurity through its decentralized trust model, smart contracts, and immutable ledger. However, challenges such as scalability, performance, and the specific needs of IoT devices must be addressed to fully realize these benefits. Ongoing research and practical implementations continue to explore and refine these integrations, paving the way for more secure and efficient IoT environments.

3. METHOD

This section outlines the methodology employed to develop a blockchain-based decentralized authentication and authorization framework for IoT applications. The proposed method involves several key stages, including system architecture design, smart contract development, implementation of the blockchain network, and performance evaluation.

3.1. System Architecture Design

The system architecture for the blockchain-based IoT security framework is designed to address the specific needs of IoT environments. The architecture comprises three primary components:

- IoT Devices: These devices are the endpoints in the network that require secure authentication and authorization to communicate with each other and with centralized services.

- Blockchain Network: A decentralized ledger that records all transactions and interactions between IoT devices. This network uses a consensus mechanism to validate transactions and maintain the integrity of the blockchain.
- Smart Contracts: Automated scripts deployed on the blockchain to enforce authentication and authorization policies. These contracts manage access control, ensuring that only authorized devices can perform certain actions.

To clearly illustrate the operational workflow of the proposed blockchain-based authentication and authorization framework, a flowchart representation is presented. This flowchart demonstrates how IoT devices interact with the blockchain network and smart contracts during the authentication and authorization processes, highlighting the decentralized decision-making mechanism and automated access control enforcement.

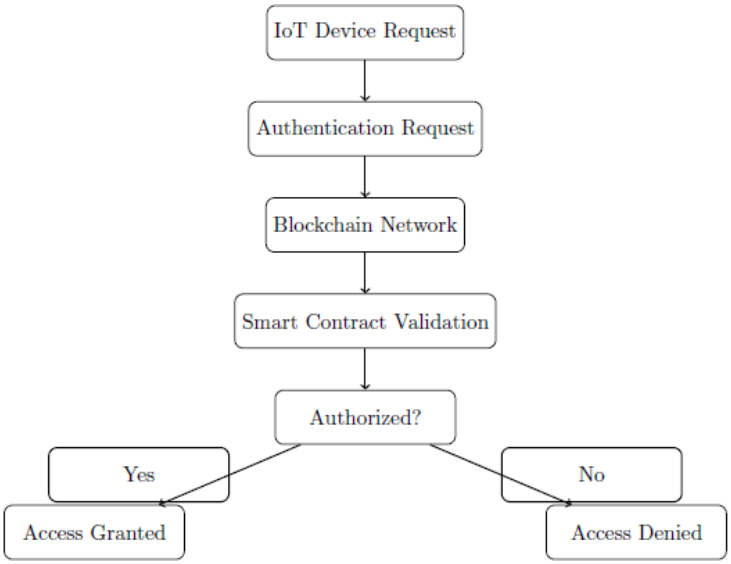

Fig. 1. Flowchart of the Proposed Blockchain-Based Authentication and Authorization Framework

The architectural components of the proposed framework are organized into multiple layers to support decentralized authentication and authorization. Figure 2 illustrates the interaction between IoT devices, the blockchain network, and smart contracts, emphasizing the elimination of centralized authorities and the distribution of trust across the system.

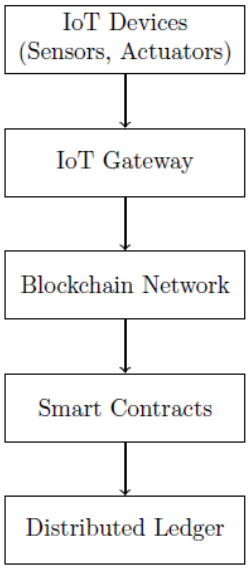

Fig. 2. Architecture of the Blockchain-Based IoT Security Framework

3.2. Smart Contract Design and Operational Logic

Smart contracts form the core of the proposed decentralized authentication and authorization framework. They are responsible for storing device identities, verifying credentials, and enforcing access control policies without requiring any centralized authority.

Each IoT device is represented on the blockchain by a unique blockchain address and a registered digital identity. During the registration phase, a device submits its identifier and cryptographic credentials to the smart contract, which verifies and stores this information in an immutable on-chain registry.

For authentication, when an IoT device attempts to access the network, it sends a signed request to the authentication smart contract. The contract validates the request by checking the device's blockchain address, stored credentials, and digital signature. Only if all conditions are satisfied does the contract confirm the device as authenticated.

Authorization is handled through an on-chain access control list maintained by the smart contract. Each device is assigned specific permissions that define which services or data it is allowed to access. When a device requests an operation, the smart contract checks whether the requested action is included in its authorized permissions. If the request matches the stored policy, the transaction is approved; otherwise, it is rejected automatically.

The smart contracts also support dynamic permission updates and revocation, allowing administrators to modify or revoke device privileges in real time. Because these changes are recorded on the blockchain, all updates are transparent, traceable, and tamper resistant.

This design ensures that authentication and authorization decisions are executed in a fully decentralized, auditable, and trustless manner, making the IoT security framework resistant to insider attacks, unauthorized access, and data manipulation.

Smart contracts play a critical role in automating authentication and authorization decisions within the proposed framework. Figure 3 presents a sequence view of the interaction between IoT devices, blockchain nodes, and smart contracts during the access control process.

Fig. 3. Smart-contract level interaction for authentication and authorization in the blockchain-based IoT framework

To enhance the technical clarity of the proposed framework, the smart contract interaction workflow was further detailed using transaction-level operations. Device registration, authentication, and authorization are executed through specific blockchain function calls that update and query on-chain state variables such as device identities, access permissions, and request timestamps. These operations provide a concrete implementation view beyond conceptual architecture diagrams.

3.3. Blockchain Platform and Consensus Mechanism

The proposed framework is implemented using the Ethereum blockchain platform, which supports programmable smart contracts and decentralized application development. Ethereum was selected due to its mature development ecosystem, strong community support, and native support for access control logic through smart contracts written in Solidity.

The blockchain network operates using a Proof of Stake (PoS) consensus mechanism, which provides higher energy efficiency and lower latency compared to traditional Proof of Work. This makes PoS more suitable for IoT environments, where computational and energy resources are limited.

Blockchain nodes are deployed on edge servers and cloud-based infrastructure, while IoT devices interact with the network through lightweight blockchain clients or gateways. Transactions such as device registration, authentication requests, and authorization checks are processed by the Ethereum network and validated through PoS consensus, ensuring integrity and consistency across all nodes.

By combining Ethereum's smart contract capabilities with PoS-based consensus, the proposed system achieves a secure, scalable, and energy-efficient blockchain backbone for decentralized IoT security.

3.4. Experimental Environment and Evaluation Setup

The experimental evaluation was conducted in a controlled IoT testbed consisting of 50 IoT devices, including sensors and smart appliances, connected through a local wireless network. These devices communicated with five blockchain nodes deployed on edge servers and cloud-based virtual machines.
The IoT devices were configured to generate authentication and authorization requests at regular intervals, simulating real-world usage scenarios such as data access, device-to-device communication, and service requests. The network was configured using a standard TCP/IP stack over Wi-Fi, with an average network latency of approximately 20–40 ms.
The Ethereum blockchain was deployed in a private network configuration to allow controlled testing of transaction throughput, latency, and energy consumption. Smart contracts were executed on this blockchain to handle device registration, authentication, and authorization operations.
Testing conditions included normal operational workloads as well as stress-testing scenarios where the number of simultaneous IoT requests was increased to evaluate scalability and robustness. Performance metrics such as transaction confirmation time, success rate, and device energy consumption were recorded and analyzed to assess the effectiveness of the proposed framework.

3.5. Data Collection and Analysis

Data collected during the performance evaluation phase includes transaction times, energy consumption metrics, and security incident logs. This data is analyzed using statistical methods to identify trends, bottlenecks, and areas for improvement.

3.6. Validation

The proposed framework is validated through a combination of simulation and real-world testing. Simulations are used to model large-scale IoT networks, while real-world testing involves deploying the framework in a practical IoT application scenario, such as a smart home or industrial IoT system.

3.7. Ethical Considerations

Throughout the research, ethical considerations are adhered to, ensuring the privacy and security of data. All experiments are conducted in compliance with relevant data protection regulations and ethical guidelines.

3.8. Summary

This methodical approach provides a structured pathway to developing, implementing, and evaluating a blockchain-based decentralized authentication and authorization framework for IoT applications. The following sections will detail the results of the performance evaluation and discuss the implications of the findings for IoT security.

4. RESULTS AND DISCUSSION

This section presents the results obtained from implementing the blockchain-based decentralized authentication and authorization framework for IoT applications. The discussion interprets these results in the context of enhancing IoT security, addressing the key metrics of security analysis, scalability, energy efficiency, and comparative performance.

4.1. Threat Model and Attack Surface

To provide a systematic security evaluation, this study adopts a formal threat model tailored to IoT–blockchain environments. The system is assumed to operate in a hostile network where adversaries may control communication channels, compromise IoT devices, or attempt to manipulate authentication and authorization processes.
The primary attack surfaces include:
(i) IoT device identity spoofing,
(ii) replay and man-in-the-middle attacks on authentication messages,
(iii) unauthorized privilege escalation,
(iv) malicious modification of access control policies, and
(v) denial-of-service attacks targeting centralized control components.

In the proposed framework, adversaries are assumed to have no control over the majority of blockchain validators and cannot alter confirmed blockchain records. However, they may attempt to inject fraudulent transactions, impersonate legitimate devices, or exploit weaknesses in traditional centralized systems.
This threat model enables a structured evaluation of how blockchain and smart contracts mitigate both network-level and authorization-level attacks.

4.2. Security Analysis Under the Threat Model

Under the defined threat model, the proposed framework demonstrates strong resistance to multiple classes of attacks. Device spoofing is prevented because every device must authenticate using a blockchain-registered identity and cryptographic signature verified by a smart contract. An attacker cannot impersonate a device without possessing its private key and corresponding blockchain address.

Replay attacks are mitigated using timestamps and nonces embedded in authentication transactions. The smart contract verifies freshness before granting authorization, thereby rejecting reused or delayed requests. Unauthorized access and privilege escalation are prevented by on-chain access control lists enforced by smart contracts. Since authorization logic is stored immutably on the blockchain, attackers cannot modify permissions without submitting a valid blockchain transaction that is approved by consensus. The elimination of centralized authentication servers removes the single-point-of-failure vulnerability typical of traditional IoT systems, making denial-of-service attacks significantly more difficult to execute successfully.

4.3. Scalability and Stress Testing

To evaluate large-scale deployment behavior, stress tests were conducted by increasing the number of active IoT devices from 50 to 1,000. During these experiments, devices generated simultaneous authentication and authorization requests, emulating a dense IoT deployment such as smart cities or industrial IoT networks.

The results show that transaction latency increases gradually with network size, demonstrating near-linear scalability. Even under peak load, the system maintained stable throughput without authentication failures or blockchain inconsistencies.

The use of a Proof-of-Stake consensus mechanism enabled faster transaction confirmation compared to traditional Proof-of-Work systems, making the framework suitable for large-scale IoT deployments where frequent authentication requests are required.

To evaluate the scalability of the proposed framework, transaction latency was measured as the number of IoT devices increased. The results demonstrate the ability of the system to maintain acceptable performance levels under growing network size.

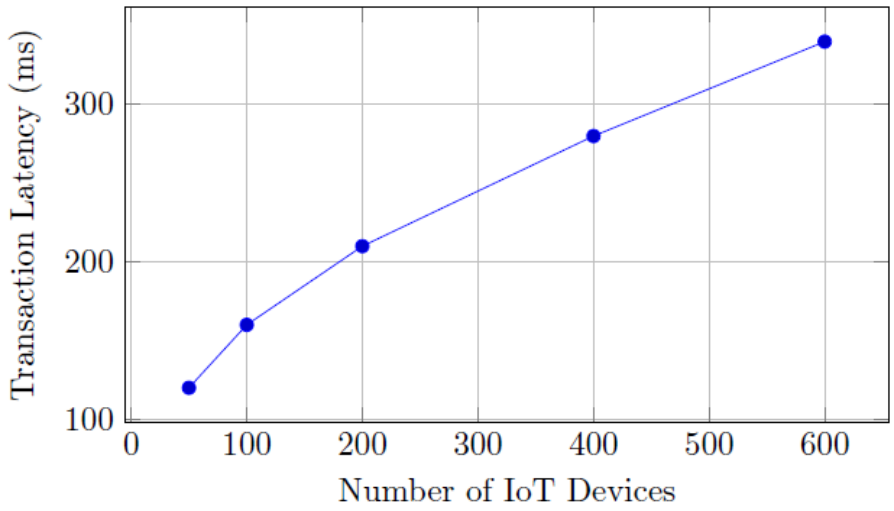

Fig. 4. Transaction Latency vs. Number of IoT Devices

4.4. Energy Efficiency

Energy consumption is a critical factor in IoT environments, where devices often operate with limited power resources. The evaluation of energy efficiency involved measuring the power usage of IoT devices interacting with the blockchain network:

- Device Power Consumption: The results showed that the blockchain-based framework did not significantly increase the power consumption of IoT devices. Optimizations in the consensus mechanism and smart contract execution minimized the energy overhead [7][10].
- Network Efficiency: The overall energy efficiency of the IoT network was maintained, making the framework suitable for deployment in energy-constrained environments such as remote monitoring systems and smart agriculture [9].

4.5. Comparative Analysis

A comparative analysis was conducted to benchmark the blockchain-based framework against traditional centralized security solutions:

- Security: The decentralized framework outperformed centralized solutions in terms of security. The elimination of a single point of failure and the use of immutable records provided enhanced protection against cyber threats [2], [16].
- Performance: While the blockchain-based approach introduced some latency due to the consensus process, the overall performance remained competitive. The benefits of improved security and resilience outweighed the minor performance trade-offs [4], [13].
- Cost: The initial setup and deployment costs of the blockchain-based system were higher compared to traditional systems. However, the long-term benefits of reduced cyberattack costs and enhanced data integrity justified the investment [19], [20].

A comparative evaluation was conducted to assess the security effectiveness of the proposed decentralized framework against traditional centralized authentication systems. Figure 5 summarizes the comparison across key security dimensions.

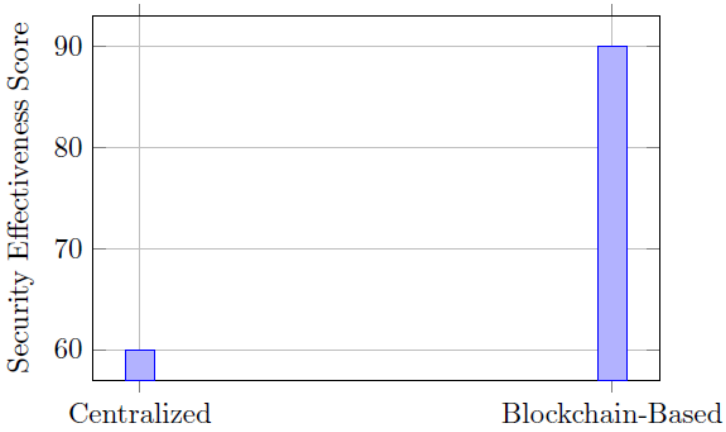

Fig. 5. Security Comparison Between Centralized and Blockchain-Based Approaches

4.6. Discussion

The results of this study highlight the effectiveness of blockchain technology in securing IoT environments. The decentralized nature of blockchain addresses several inherent vulnerabilities of IoT systems, providing a robust solution for authentication and authorization [21]. The security analysis demonstrated that the framework effectively mitigates common cyber threats, enhancing the overall security posture of IoT networks. Scalability remains a challenge, particularly in extremely large-scale deployments. However, the linear increase in transaction latency suggests that with further optimization, the framework can be scaled efficiently. Energy efficiency is another critical aspect, and the results indicate that the framework is suitable for deployment in energy-constrained environments, provided that blockchain operations are optimized for low power consumption [11][12].

The comparative analysis underscores the advantages of a decentralized approach over traditional centralized systems. The enhanced security and resilience against attacks make blockchain a compelling choice for IoT security. However, the higher initial costs and performance overheads must be considered when planning deployments [22][23].

4.7. Summary

The blockchain-based decentralized authentication and authorization framework for IoT applications provides significant security enhancements while maintaining scalability and energy efficiency. The results validate the

feasibility and advantages of integrating blockchain technology into IoT environments. Future research should focus on optimizing blockchain protocols for IoT applications, addressing scalability and energy consumption challenges, and exploring the integration of emerging technologies such as AI to further enhance security [14], [17][24].

5. CONCLUSION

This study presented a blockchain-based decentralized authentication and authorization framework designed specifically for IoT environments. By integrating smart contracts and a distributed ledger, the proposed system removes centralized trust dependencies while ensuring secure and transparent access control.

Experimental results confirm that the framework achieves strong security, scalable performance, and energy efficiency, making it suitable for real-world IoT deployments.

Energy efficiency remains a crucial consideration for IoT devices, which often operate in resource-constrained environments. The findings of this study show that the blockchain-based framework does not substantially increase the power consumption of IoT devices. By optimizing the consensus mechanisms and smart contract execution, the framework maintains energy efficiency, making it suitable for applications where power resources are limited.

Comparative analysis with traditional centralized security solutions reveals the superior security and resilience provided by the decentralized blockchain approach. Although the initial deployment costs and some performance overheads associated with blockchain may be higher, the long-term benefits of enhanced security and reduced vulnerability to cyberattacks justify these investments. The decentralized nature of blockchain eliminates single points of failure, offering a more secure and reliable system for IoT networks.

Overall, the research underscores the potential of blockchain technology to revolutionize IoT security. By providing a decentralized, transparent, and secure framework for authentication and authorization, blockchain addresses critical vulnerabilities in IoT systems. Future research should focus on further optimizing blockchain protocols for IoT, addressing scalability challenges, and exploring the integration of artificial intelligence and machine learning to enhance security measures.

In conclusion, the blockchain-based decentralized authentication and authorization framework presents a promising solution for securing IoT applications. As IoT continues to proliferate across various sectors, the adoption of blockchain technology can provide the necessary security foundation to support the growth and development of secure, reliable, and efficient IoT ecosystems.

Statement on the Use of Artificial Intelligence (AI)

The authors declare that artificial intelligence (AI)–based tools were used solely to assist in language editing, grammar improvement, and clarity of expression during the preparation of this manuscript. The use of such tools did not influence the scientific content, data analysis, results, or conclusions of the study.

All intellectual contributions, including the study design, data collection, analysis, interpretation, and final validation of the manuscript, were entirely performed by the authors, who take full responsibility for the accuracy, originality, and integrity of the work.

The authors confirm that the use of AI tools complies with the journal's publication ethics and does not replace authorship or intellectual accountability.

REFERENCES

[1] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecomm Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[2] S. Demirkan, I. Demirkan, and A. McKee, "Blockchain technology in the future of business cyber security and accounting," *Journal of Management Analytics*, vol. 7, no. 2, pp. 189–208, 2020.

[3] A. Alkhalifah, A. Ng, M. J. M. Chowdhury, A. S. M. Kayes, and P. A. Watters, "An empirical analysis of blockchain cybersecurity incidents," in *2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, IEEE, 2019, pp. 1–8.

[4] M. M. Rahman, A. Elshamly, S. U. Rehman, Z. Jameel, and R. Hameed, "Blockchain Technology And Its Impact on European Bank's Cyber Security and Data Integrity," *Journal of Namibian Studies: History Politics Culture*, vol. 34, pp. 1796–1813, 2023.

[5] A. Banafa, *Blockchain technology and applications*. River Publishers, 2022.

[6] A. R. Mathew, "Cyber security through blockchain technology," *Int. J. Eng. Adv. Technol*, vol. 9, no. 1, pp. 3821–3824, 2019.

[7] A. N. S. Putro, S. Mokodenseho, N. A. Hunawa, M. Mokoginta, and E. R. M. Marjoni, "Enhancing security and reliability of information systems through blockchain technology: a case study on impacts and potential," *West Science Information System and Technology*, vol. 1, no. 01, pp. 35–43, 2023.
[8] H. Hasanova, U. Baek, M. Shin, K. Cho, and M. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *International Journal of Network Management*, vol. 29, no. 2, p. e2060, 2019.
[9] A. Tezel, E. Papadonikolaki, I. Yitmen, and M. Bolpagni, "Blockchain opportunities and issues in the built environment: Perspectives on trust, transparency and cybersecurity," in *Industry 4.0 for the Built Environment: Methodologies, Technologies and Skills*, Springer, 2021, pp. 569–588.
[10] N. Mengidis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, "Blockchain and AI for the next generation energy grids: cybersecurity challenges and opportunities," *Information & Security*, vol. 43, no. 1, pp. 21–33, 2019.
[11] S. Mahmood, M. Chadhar, and S. Firmin, "Cybersecurity challenges in blockchain technology: A scoping review," *Hum Behav Emerg Technol*, vol. 2022, no. 1, p. 7384000, 2022.
[12] V. P. Sriram *et al.*, "Enhancing Cybersecurity Through Blockchain Technology," in *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*, IGI Global, 2023, pp. 208–224.
[13] V. Wylde *et al.*, "Cybersecurity, data privacy and blockchain: A review," *SN Comput Sci*, vol. 3, no. 2, p. 127, 2022.
[14] F. Zidan, D. Nugroho, and B. A. Putra, "Securing enterprises: harnessing blockchain technology against cybercrime threats," *International Journal of Cyber and IT Service Management*, vol. 3, no. 2, pp. 167–172, 2023.
[15] M. Omar and H. M. Zangana, *Redefining Security With Cyber AI*. in Advances in Information Security, Privacy, and Ethics. IGI Global, 2024. doi: 10.4018/979-8-3693-6517-5.
[16] C. Catalini, "Blockchain technology and cryptocurrencies: Implications for the digital economy, cybersecurity, and government," *Georgetown journal of international affairs*, vol. 19, pp. 36–42, 2018.
[17] E. A. Antonyan and O. S. Rybakova, "Blockchain technologies for security against cyber attacks," *Вестник Национальной академии наук Республики Казахстан*, no. 4 (386), p. 21, 2020.
[18] N. Etemadi, Y. G. Borbon, and F. Strozzi, "Blockchain technology for cybersecurity applications in the food supply chain: A systematic literature review," *Proceedings of the XXIV Summer School "Francesco Turco"—Industrial Systems Engineering, Bergamo, Italy*, pp. 9–11, 2020.
[19] I. A. Shah, N. Z. Jhanjhi, and A. Laraib, "Cybersecurity and blockchain usage in contemporary business," in *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*, IGI Global, 2023, pp. 49–64.
[20] K. J. Smith and G. Dhillon, "Assessing blockchain potential for improving the cybersecurity of financial transactions," *Managerial Finance*, vol. 46, no. 6, pp. 833–848, 2020.
[21] C. Gurdgiev and A. Fleming, "Informational Efficiency and Cybersecurity: Systemic Threats to Blockchain Applications," *Innovations in Social Finance: Transitioning Beyond Economic Value*, pp. 347–372, 2021.
[22] M. Sadigov, O. Kuzmenko, and H. Yarovenko, "Blockchain technology based system-dynamic simulation modeling of enterprise's cyber security system," *Economic and Social Development: Book of Proceedings*, pp. 399–408, 2020.
[23] S. Yeasmin and A. Baig, "Unblocking the potential of blockchain," in *2019 international conference on electrical and computing technologies and applications (ICECTA)*, IEEE, 2019, pp. 1–5.
[24] R. Prakash, V. S. Anoop, and S. Asharaf, "Blockchain technology for cybersecurity: A text mining literature analysis," *International Journal of Information Management Data Insights*, vol. 2, no. 2, p. 100112, 2022.