Vol 2 No 3 2025 || E-ISSN 2997-7258

The Journal of Academic Science

journal homepage:
https://thejoas.com/index.php/

Blockchain-Powered Security Framework for IoT Data Integrity and Privacy

Asep Arwan Sulaeman
Universitas Pelita Bangsa, Indonesia
Email: aseparwan@pelitabangsa.ac.id

KEY W O R D S
Blockchain
Security,
IoT Data Integrity,
Privacy Protection,
Smart Contracts,
Decentralized
Trust.

A B S T R A C T
The rapid expansion of the Internet of Things (IoT) has introduced significant challenges regarding data integrity and privacy. Traditional security mechanisms often fail to address the vulnerabilities associated with decentralized and resource-constrained IoT environments. This study proposes a Blockchain-Powered Security Framework to enhance the integrity and privacy of IoT data. Using a qualitative research methodology, including literature review and library research, this paper explores the feasibility of blockchain technology in mitigating IoT security threats. The study examines existing blockchain-based security solutions and evaluates their effectiveness in ensuring data confidentiality, authentication, and tamper resistance. Findings indicate that blockchain's decentralized nature, cryptographic hashing, and smart contracts can significantly enhance IoT security by providing immutable data records, decentralized trust management, and autonomous execution of security policies. Furthermore, this research identifies key challenges such as scalability, energy efficiency, and regulatory constraints that must be addressed for widespread adoption. The study highlights that integrating lightweight consensus mechanisms and off-chain storage can optimize blockchain implementation in IoT networks. By synthesizing insights from existing literature, this research contributes to the development of a secure and privacy-preserving IoT ecosystem. The proposed framework emphasizes a multi-layered security approach that integrates blockchain with cryptographic techniques, ensuring robust defense against cyber threats. This study underscores the importance of further empirical validation and regulatory advancements to facilitate the practical implementation of blockchain-powered IoT security frameworks. Future research should focus on optimizing blockchain architectures tailored for IoT environments to achieve a balance between security, efficiency, and scalability.

1. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has revolutionized multiple industries, including healthcare, transportation, and smart cities. However, the increasing number of connected devices has raised serious concerns regarding data integrity, security, and privacy (Mehta & Kumar, 2024). Traditional security mechanisms, such as centralized authentication and encryption protocols, have proven inadequate in addressing IoT-related vulnerabilities due to their centralized nature and susceptibility to cyberattacks (Salama et al., 2024). Blockchain technology has emerged as a promising solution, offering a decentralized, tamper-proof, and transparent security mechanism that ensures the integrity and confidentiality of IoT data (Raza & Molloholli, 2024). Despite its potential, the implementation

of blockchain in IoT ecosystems remains challenging due to scalability issues, energy consumption, and computational constraints (Dhatterwal et al., 2025).

Existing studies have explored blockchain-based security frameworks for IoT; however, most focus on theoretical models rather than practical implementation and performance evaluation (Santhiyakumari, 2024). Moreover, prior research often addresses specific security aspects such as authentication or data integrity without considering a holistic framework integrating blockchain with cryptographic techniques (Mehta et al., 2024). Additionally, current blockchain-powered IoT security models lack comprehensive strategies for mitigating scalability and efficiency trade-offs (RosarioGilmary et al., 2024). This research addresses these gaps by developing a multi-layered blockchain-based security framework tailored to IoT applications, ensuring improved privacy protection, data integrity, and decentralized trust management.

As IoT adoption continues to grow, the need for robust security frameworks becomes increasingly urgent. Cyber threats such as data breaches, unauthorized access, and malicious node attacks pose significant risks to IoT ecosystems (Mehta & Singh, 2024). Addressing these challenges is critical to ensuring the secure deployment of IoT technologies across critical sectors such as healthcare, finance, and smart cities (Salama et al., 2024). Given the limitations of existing security solutions, blockchain offers a viable approach to enhancing IoT security while maintaining efficiency and scalability.

Several studies have investigated the integration of blockchain technology into IoT security. Raza & Molloholli (2024) proposed a blockchain-powered security model for safeguarding IoT ecosystems but did not address the computational overhead associated with blockchain implementation. Dhatterwal et al. (2025) explored decentralized data management for IoT but lacked considerations for lightweight consensus mechanisms. RosarioGilmary et al. (2024) introduced a blockchain-powered vehicular communication security framework, focusing primarily on data transmission integrity rather than a comprehensive IoT security model. This research builds upon these studies by designing an optimized blockchain-based security framework that balances security, efficiency, and scalability.

The novelty of this research lies in the development of a multi-layered blockchain security framework specifically designed for IoT environments. Unlike existing models, this framework integrates lightweight consensus mechanisms, cryptographic enhancements, and off-chain storage solutions to mitigate performance bottlenecks associated with blockchain adoption in IoT networks (Santhiyakumari, 2024). Additionally, the study proposes a hybrid blockchain structure that combines public and private blockchain features, ensuring enhanced security without compromising efficiency (Mehta et al., 2024). This study aims to:

1. Develop a blockchain-powered security framework to enhance data integrity and privacy in IoT ecosystems.
2. Analyze the feasibility of blockchain adoption in IoT applications by evaluating security, efficiency, and scalability trade-offs.
3. Propose cryptographic optimizations and lightweight consensus mechanisms to improve blockchain-based IoT security

models.
4. Assess the framework's effectiveness through comparative analysis with existing security approaches.

The findings of this research contribute to both theoretical and practical advancements in IoT security. From an academic perspective, the study expands the knowledge base on blockchain-powered security frameworks, offering new insights into their practical applicability in IoT ecosystems (RosarioGilmary et al., 2024). From an industry perspective, the proposed security framework provides enhanced data integrity, privacy protection, and decentralized trust management, ensuring safer IoT deployments across various sectors (Mehta & Singh, 2024). This research will be beneficial to cybersecurity practitioners, IoT developers, and policymakers seeking robust security solutions for emerging IoT technologies.

2. METHOD

This study employs a qualitative research methodology with a literature review (library research) approach to examine the role of blockchain technology in enhancing IoT data integrity and privacy. The qualitative method allows for an in-depth exploration of blockchain's potential, limitations, and implementation strategies in IoT ecosystems (Chaganti, 2024). By synthesizing existing academic literature, this research aims to develop a comprehensive understanding of blockchain-based security frameworks and their applicability in real-world IoT environments.

The data sources for this study include peer-reviewed journal articles, conference proceedings, and technical reports published within the last five years. These sources are obtained from reputable digital libraries, including IEEE Xplore, Springer, Elsevier, and Google Scholar (Sawai & Chakravarthi, 2025). The selected studies focus on blockchain applications in IoT security, covering topics such as decentralized trust management, data privacy, cryptographic mechanisms, and lightweight consensus algorithms (Roy, 2024). This approach ensures that the research is grounded in current and relevant scholarly contributions.

The data collection technique employed in this study is document analysis, where selected literature is reviewed systematically to identify key themes, trends, and research gaps. The selection criteria include publication recency, relevance to blockchain-based IoT security, and methodological rigor (Nasution, 2024). To enhance reliability, multiple independent sources are cross-examined to validate findings and reduce potential biases (Mahesha, 2024).

The data analysis method involves a thematic analysis approach, where identified studies are categorized based on their contributions to IoT security, blockchain architecture, and emerging challenges (Celestin, 2024). This process involves coding and clustering relevant information to identify patterns and correlations across different studies (Ajakwe et al., 2024). Thematic synthesis is then used to formulate a blockchain-powered security framework tailored for IoT environments, ensuring robust data protection and privacy mechanisms (Negi, 2024). This methodological approach provides a structured and evidence-based understanding of blockchain's role in mitigating IoT security threats, contributing to both theoretical advancements and practical applications.

3. RESULT AND DISCUSSION

The following table presents the findings from a literature review on blockchain-powered security frameworks for IoT data integrity and privacy. The data consists of 10 selected articles from the last five years, obtained from Google Scholar. These articles were filtered based on their relevance, recency, and contribution to the research topic.

Table 1 Literature Review

No	Author(s) & Year	Title	Key Findings
1	RosarioGilmary & JayasriS (2024)	Blockchain-Powered Security Management System for Vehicular Communication	Blockchain improves data transmission security in vehicular communication.
2	Mehta & Singh (2024)	Blockchain-Powered Federated Learning: A Secure and Decentralized Approach to Distributed AI	Federated learning combined with blockchain enhances privacy and trust in decentralized AI.
3	Raza & Molloholli (2024)	Blockchain-Powered Security Solutions for Safeguarding IoT Ecosystems	Blockchain secures IoT ecosystems with decentralized trust and cryptographic mechanisms.
4	Dhatterwal et al. (2025)	Decentralized Data Management for CIoT Using Blockchain Technology	Decentralized data management reduces risks of data breaches and enhances security.
5	Salama et al. (2024)	6G Networks Powered by Blockchain Technology for Intelligent Medical Applications	Blockchain enhances data integrity in medical applications using 6G networks.
6	Mehta & Kumar (2024)	Blockchain-powered Solutions for Ensuring IoVT Data Confidentiality and Integrity	IoVT security benefits from blockchain, mitigating unauthorized access risks.
7	Santhiyakumari (2024)	Blockchain-Powered Secure Communication Protocol for the Internet of Medical Things (IoMT)	Blockchain strengthens IoMT data privacy, securing medical data transmission.

8	Sawai & Chakravarthi (2025)	Scalability and Performance of Blockchain-Based Solutions for IoT Applications	Scalability and performance optimization of blockchain in IoT networks.
9	Negi (2024)	Towards the Integration of IT/OT Technologies in Electricity-Based Digitalized Energy Systems	Integrating IT and OT for digitalized energy systems with blockchain security.
10	Celestin (2024)	Monetizing IoT Data: Blockchain's Role in Creating New Business Models	Monetization strategies for IoT data using blockchain technology.

The selected literature provides valuable insights into the application of blockchain-powered security frameworks for ensuring IoT data integrity and privacy. The studies collectively highlight the transformative role of decentralized ledger technology in mitigating cybersecurity vulnerabilities inherent in IoT ecosystems. One key observation across multiple studies is that blockchain's immutability and cryptographic mechanisms offer a robust solution for securing IoT data transmission (RosarioGilmary & JayasriS, 2024). The integration of blockchain technology ensures tamper-proof records and prevents unauthorized modifications, which is a critical advantage in sectors such as healthcare, transportation, and smart cities.

A major area of emphasis in recent research is the combination of blockchain with federated learning and artificial intelligence (AI) models (Mehta & Singh, 2024). This approach enhances privacy-preserving machine learning applications in decentralized networks, ensuring that sensitive data remains confidential while allowing for collaborative intelligence across IoT devices. Such an approach is particularly relevant in environments where data sovereignty and user privacy are critical concerns, such as in medical IoT (IoMT) and industrial IoT (IIoT) applications.

Another key finding in the literature is the importance of decentralized trust management within IoT ecosystems. Traditional centralized security architectures pose risks of single points of failure, making IoT networks vulnerable to cyberattacks (Raza & Molloholli, 2024). By adopting blockchain-based identity authentication and distributed consensus mechanisms, IoT devices can achieve trustless security models that mitigate fraud, impersonation, and unauthorized access attempts. This decentralized authentication system significantly reduces reliance on third-party security providers, enhancing both security and operational efficiency.

However, blockchain's integration with IoT networks is not without its challenges. One of the major hurdles identified in multiple studies is scalability and performance optimization (Sawai & Chakravarthi, 2025). The computational

overhead and high energy consumption associated with Proof-of-Work (PoW) or even some Proof-of-Stake (PoS) consensus mechanisms can hinder blockchain's feasibility in resource-constrained IoT environments. Researchers have proposed lightweight consensus algorithms and off-chain data storage solutions to optimize blockchain deployment in IoT systems, reducing latency and improving transaction throughput.

The medical and healthcare sectors have also emerged as a high-impact application area for blockchain-powered IoT security frameworks. Blockchain solutions are being explored for ensuring data integrity in electronic health records (EHRs), securing remote patient monitoring (RPM) systems, and protecting medical IoT devices from cyber threats (Salama et al., 2024). The integration of 6G networks with blockchain technology has been suggested as a next-generation security paradigm that will enhance privacy protection and high-speed encrypted communication between IoT-enabled healthcare devices.

Finally, a growing body of research focuses on the economic implications of blockchain-powered IoT security solutions. Blockchain facilitates new monetization strategies for IoT data, enabling secure data marketplaces where entities can buy, sell, and exchange data with transparency and security (Celestin, 2024). The ability to tokenize IoT-generated data assets while ensuring data provenance and authenticity could unlock new business models for companies looking to capitalize on trusted data transactions.

The increasing reliance on Internet of Things (IoT) devices across multiple industries has amplified concerns regarding data integrity, security, and privacy. As IoT ecosystems expand, high-profile cyberattacks such as ransomware attacks on critical infrastructure, data breaches in healthcare, and smart city surveillance vulnerabilities underscore the urgent need for robust security frameworks. The selected literature highlights how blockchain technology serves as a viable solution to mitigate these security risks by providing decentralized, immutable, and transparent data management mechanisms (RosarioGilmary & JayasriS, 2024). The rise of state-sponsored cyber threats and AI-driven hacking techniques further emphasizes the necessity of adopting next-generation security solutions like blockchain.

One of the most pressing global concerns today is the increasing sophistication of cyberattacks targeting IoT devices in smart homes, industrial control systems (ICS), and autonomous vehicles. The literature review reveals that blockchain-powered security mechanisms can effectively counteract these threats by eliminating single points of failure in IoT networks (Raza & Molloholli, 2024). For instance, in autonomous vehicles and connected transportation networks, blockchain can validate communication between vehicles, traffic systems, and IoT-enabled infrastructure, thereby reducing risks of hacking-induced accidents and system failures. Given the rising incidents of autonomous vehicle hacking in countries like the United States and China, implementing blockchain as a trust verification system is becoming increasingly relevant.

Another critical phenomenon is the rapid adoption of AI and machine learning in IoT applications, particularly in healthcare, finance, and manufacturing. The integration of blockchain with federated learning models, as highlighted in Mehta & Singh (2024), provides a privacy-preserving AI framework where data can

be analyzed locally on IoT devices without centralizing sensitive information. This is particularly crucial in the medical IoT (IoMT) sector, where the security of patient records and remote health monitoring systems has become a top priority due to the surge in telemedicine and digital health adoption post-COVID-19. The increasing cyberattacks on hospitals and medical databases further validate the necessity of blockchain-based IoT security frameworks to ensure tamper-proof patient data management.

The growing focus on data sovereignty and compliance with regulations such as General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA), and China's Data Security Law (DSL) presents another major challenge for IoT security. Blockchain's smart contract functionality offers an opportunity to automate regulatory compliance and data governance policies (Salama et al., 2024). As governments enforce stricter data protection laws, blockchain-powered solutions can help IoT service providers ensure compliance while maintaining user privacy and data transparency. The increasing debate over data ownership, particularly in smart cities and digital identities, has made blockchain a critical enabler of self-sovereign identity (SSI) models, reducing reliance on centralized identity providers.

In the energy sector, the transition toward smart grids and decentralized energy systems highlights the need for secure IoT infrastructure. Blockchain has been identified as a key technology in securing energy trading systems, ensuring transparent electricity consumption tracking, and mitigating cyber risks in power grids (Negi, 2024). With the rise of cyberattacks on energy infrastructure, such as the Colonial Pipeline ransomware attack in 2021, blockchain-powered security frameworks are increasingly being explored to fortify energy grids and renewable energy systems against cyber threats. This aligns with global sustainability efforts, as blockchain can enhance trust in carbon credit trading and decentralized renewable energy markets.

Furthermore, the monetization of IoT-generated data is becoming an increasingly profitable yet risky market, as seen in the surge of data marketplaces and real-time data analytics platforms. Blockchain facilitates secure data transactions where businesses and individuals can trade IoT data transparently without the risk of data manipulation (Celestin, 2024). This is particularly relevant in the industrial IoT (IIoT) and agriculture IoT (AgriTech) sectors, where data collected from smart sensors is used for predictive maintenance, crop monitoring, and supply chain optimization. The increasing value of IoT data, coupled with concerns over data misuse and unauthorized selling of consumer information, makes blockchain-powered data integrity solutions essential.

4. CONCLUSION

The findings from this literature review confirm that blockchain-powered security frameworks offer a promising solution to address IoT data integrity and privacy concerns. The reviewed studies highlight that decentralized trust mechanisms, cryptographic hashing, and immutable ledger technology enhance IoT security by preventing unauthorized access, data manipulation, and cyberattacks. The integration of blockchain with federated learning, smart contracts, and lightweight consensus mechanisms further strengthens IoT security models, particularly in healthcare, smart cities, and industrial IoT environments. However,

despite these advancements, challenges such as scalability limitations, high computational overhead, and regulatory constraints remain key barriers to large-scale blockchain adoption in IoT networks.

In light of current technological trends, blockchain-powered security frameworks are becoming increasingly relevant and necessary due to the growing cyber threats targeting IoT devices, the need for regulatory compliance, and the rising monetization of IoT-generated data. The literature suggests that implementing hybrid blockchain models that integrate both public and private blockchain features can enhance efficiency, security, and scalability. Additionally, blockchain's role in self-sovereign identity management and decentralized data marketplaces presents new opportunities for ensuring data ownership, transparency, and trust. As industries increasingly depend on IoT ecosystems, blockchain's role in secure data transmission, authentication, and encryption will be pivotal in fortifying critical infrastructure and digital systems.

Future research should focus on real-world case studies and experimental implementations of blockchain-powered IoT security frameworks in diverse applications such as autonomous vehicles, smart healthcare, and decentralized energy systems. Additionally, further exploration into lightweight and energy-efficient blockchain protocols is necessary to overcome computational and scalability limitations. Researchers should also investigate interoperability solutions between blockchain and existing cloud-based and edge computing security frameworks to create more seamless and adaptive security architectures. Lastly, an in-depth study on the economic viability and cost-effectiveness of blockchain adoption in IoT is crucial to determine its long-term sustainability and practical deployment in industrial and consumer applications.

5. REFERENCES

Ajakwe, S. O., Saviour, I. I., & Ihekoronye, V. U. (2024). Medical IoT Record Security and Blockchain: Systematic Review of Milieu, Milestones, and Momentum. MDPI. https://www.mdpi.com/2504-2289/8/9/121

Celestin, P. (2024). Monetizing IoT Data: Blockchain's Role in Creating New Business Models. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5031247

Chaganti, K. C. (2024). Advancing AI-Driven Threat Detection in IoT Ecosystems: Addressing Scalability, Resource Constraints, and Real-Time Adaptability. TechRxiv. https://www.techrxiv.org/doi/full/10.36227/techrxiv.173738307.73168902

Dhatterwal, J. S., Kaswan, K. S., & Malik, K. (2025). Decentralized Data Management for CIoT Using Blockchain Technology. IGI Global. https://www.igi-global.com/chapter/decentralized-data-management-for-ciot-using-blockchain-technology/362546

Mahesha, V. (2024). Technological Disruption: Unraveling the Impact of AI, Blockchain, and IoT on Entrepreneurship and Industry Evolution. ResearchGate. https://www.researchgate.net/publication/378347413

Mehta, S., & Kumar, R. (2024). Blockchain-powered Solutions for Ensuring IoVT Data Confidentiality and Integrity. IEEE. https://ieeexplore.ieee.org/abstract/document/10739157/

Mehta, S., & Singh, A. (2024). Blockchain-Powered Federated Learning: A Secure and Decentralized Approach to Distributed AI. IEEE. https://ieeexplore.ieee.org/abstract/document/10896016/

Nasution, M. I. P. (2024). Analysis of Challenges and Opportunities in the Development of Information and Communication Technology in the Digital Era. Jurnal Ilmiah. https://www.ejurnal.kampusakademik.co.id/index.php/jiem/article/view/3018

Negi, M. (2024). Towards the Integration of IT/OT Technologies in Electricity-Based Digitalized Energy Systems. University of Vaasa. https://osuva.uwasa.fi/handle/10024/18361

Raza, O., & Molloholli, M. (2024). Blockchain-Powered Security Solutions for Safeguarding IoT Ecosystems. ResearchGate. https://www.researchgate.net/publication/389330549

RosarioGilmary, J., & JayasriS, S. (2024). Blockchain-Powered Security Management System for Vehicular Communication. IEEE. https://ieeexplore.ieee.org/abstract/document/10895814/

Roy, S. N. (2024). Design and Implementation of a Secure Digital Communication Protocol for IoT Devices Using Blockchain Technology. JCTMG. https://www.jctmg.in/wp-content/uploads/2024/12/IJCST-001-1-33.pdf

Salama, R., Alturjman, S., & Al-Turjman, F. (2024). 6G Networks Powered by Blockchain Technology for Intelligent Medical Applications. AI & IoT Journal. https://dergi.neu.edu.tr/index.php/aiit/article/view/924

Santhiyakumari, N. (2024). Blockchain-Powered Secure Communication Protocol for the Internet of Medical Things (IoMT). Journal of Information Technology and Digital World. https://irojournals.com/itdw/article/view/6/2/5

Sawai, N. M., & Chakravarthi, M. K. (2025). Scalability and Performance of Blockchain-Based Solutions for IoT Applications. IGI Global. https://www.igi-global.com/chapter/scalability-and-performance-of-blockchain-based-solutions-for-iot-applications/365809.