Jurnal Teknik Informatika dan Teknologi Informasi
Volume. 5 Nomor. 3 Desember 2025
E-ISSN .: 2827-9387, P-ISSN .: 2827-9379, Hal 609-621
DOI: https://doi.org/10.55606/jutiti.v5i3.6460
Tersedia: https://journalshub.org/index.php/jutiti

The Role of Blockchain in Securing Internet of Things (IoT) Ecosystems: A Cross Industry Analysis

Mega Angkasa[1*], Ika Rosalika[2], Dante Rio Sebastian[3], Beni Rahmatullah[4]
[1-4]Universitas Bina Sarana Informatika, Indonesia
mega.mea@bsi.ac.id[1], ika.iok@bsi.ac.id[2], dante.dre@bsi.ac.id[3], beni.brh@bsi.ac.id[4]
Corresponding Author: angkasamega68@gmail.com

***Abstract**. The rapid growth of the Internet of Things (IoT) has increased system connectivity across industries while simultaneously intensifying cybersecurity risks related to data integrity, access control, and system resilience. This study aims to analyze the role of blockchain technology in securing IoT ecosystems through a cross-industry perspective. A quantitative comparative approach was employed using a structured survey distributed to organizations in the manufacturing, healthcare, energy, logistics, and smart infrastructure sectors. Data were analyzed using descriptive and inferential statistical techniques to examine the effect of blockchain-based security mechanisms on IoT security performance. The findings indicate that blockchain adoption has a positive and significant impact on improving data integrity, strengthening access control, and enhancing system resilience across all observed industries. Variations in the strength of these effects reflect differences in regulatory pressure and operational risk among sectors. The results confirm that blockchain functions not only as a technical security solution but also as a strategic infrastructure for decentralized trust and risk governance in IoT environments. This study provides both theoretical contributions to IoT security frameworks and practical guidance for cross-sector blockchain implementation.*

***Keywords**: Blockchain; Cybersecurity; Cross Industry; Internet of Things; System Resilience*

1. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has fundamentally transformed industrial operations, urban infrastructure, healthcare systems, transportation networks, and digital commerce. Billions of interconnected devices now continuously generate, transmit, and process vast volumes of sensitive data across heterogeneous networks. While this pervasive connectivity enables unprecedented automation, efficiency, and real-time decision-making, it simultaneously exposes IoT ecosystems to escalating security threats. Cyberattacks such as data manipulation, identity spoofing, distributed denial of service attacks, and unauthorized device access increasingly compromise system reliability and user trust. The centralized security architectures traditionally used in IoT networks face inherent limitations related to single points of failure, limited scalability, opaque data governance, and high vulnerability to coordinated attacks.

Recent studies emphasize that the complexity and distributed nature of IoT environments demand security models that are adaptive, decentralized, and capable of maintaining integrity across diverse nodes. Conventional cryptographic approaches, while essential, often struggle to address trust management, device authentication, and immutable data logging at scale. As a response to these structural weaknesses, blockchain technology has emerged as a promising security backbone for IoT ecosystems. Its decentralized ledger

Naskah Masuk: 24 Oktober 2025; Revisi: 20 November 2025; Diterima: 18 Desember 2025; Tersedia: 24 Desember 2025

structure, cryptographic consensus mechanisms, immutability, and transparent verification processes offer a fundamentally different paradigm for securing distributed systems. Blockchain enables secure peer-to-peer transactions without centralized intermediaries, ensuring data integrity, accountability, and traceability across IoT networks.

Scholars have increasingly explored blockchain based IoT security frameworks across individual domains such as smart grids, healthcare monitoring systems, industrial automation, and supply chain management. These studies demonstrate tangible improvements in device authentication, access control, secure data exchange, and system resilience against cyber threats. Nevertheless, much of the existing literature remains sector-specific and technically fragmented, often focusing on performance optimization, consensus protocols, or isolated architectural models. Limited attention has been given to a systematic, cross industry evaluation of how blockchain reshapes security governance across diverse IoT ecosystems with varying regulatory, operational, and risk profiles.

This fragmented focus creates a significant research gap in understanding the transferability, scalability, and comparative effectiveness of blockchain-based security mechanisms across multiple industries. Each sector exhibits distinct security priorities, latency requirements, compliance obligations, and infrastructure constraints. Without a cross-industry analytical perspective, the broader strategic value of blockchain in establishing universal security standards for IoT remains underdeveloped. This limitation constrains policymakers, system architects, and industry leaders in formulating integrated security strategies that transcend sectoral boundaries.

Based on this gap, the present study is positioned to provide a comprehensive cross-industry analysis of blockchain's role in securing IoT ecosystems. The research examines how blockchain-enhanced security architectures operate across different industrial contexts, identifies shared security functions and sector specific adaptations, and evaluates the strategic implications for scalability, interoperability, and governance. The objective of this research is to develop an integrated analytical framework that clarifies how blockchain contributes to strengthening trust, resilience, and transparency in IoT ecosystems across multiple industries. Through this approach, the study seeks to advance both theoretical understanding and practical guidance for the future design of secure, decentralized IoT infrastructures.

2. LITERATURE REVIEW

The security of Internet of Things (IoT) ecosystems is fundamentally grounded in theories of distributed systems, information security governance, and trust management in networked environments (Ali et al., 2021; Dai et al., 2021). IoT architecture is inherently decentralized at the device level but often relies on centralized servers for data processing and control, creating structural vulnerabilities associated with single points of failure (Chen et al., 2021). According to distributed systems theory, network resilience increases when control and data validation are dispersed across multiple autonomous nodes (Dai et al., 2021). This theoretical foundation aligns closely with blockchain principles, where decentralization, consensus-based validation, and fault tolerance are core mechanisms for maintaining system integrity in hostile digital environments (Yang et al., 2022;Tang 2021).

From the perspective of information security theory, the classical triad of confidentiality, integrity, and availability serves as the primary benchmark for evaluating secure systems (Ferrag et al., 2020). IoT environments pose unique challenges to this triad due to constrained device resources, massive data flows, and real time operational requirements (Xu et al.,2020; Hannan et al., 2022). Blockchain technology contributes directly to the integrity dimension through its immutable ledger structure, where cryptographically linked blocks prevent unauthorized data alteration (Novo, 2020). Availability is strengthened through distributed consensus mechanisms that eliminate reliance on a single controlling authority, while confidentiality is supported through public key cryptography and permissioned access models. These characteristics position blockchain as a structural enhancement to conventional IoT security frameworks rather than merely a complementary encryption tool (Yang et al., 2022).

Trust theory in digital networks further explains the relevance of blockchain for IoT security (Makhdoom et al., 2021). Traditional trust models depend heavily on centralized certification authorities and institutional intermediaries (Novo, 2020). In large scale IoT ecosystems involving multiple vendors, operators, and jurisdictions, centralized trust infrastructures often face coordination failures and asymmetric information risks. Blockchain introduces a trustless trust model in which transactional validity is ensured through algorithmic consensus instead of institutional arbitration. This transformation shifts the foundation of trust from organizational reputation to mathematically verifiable processes, enabling secure interaction among heterogeneous and previously untrusted IoT actors (Ali et al., 2021).

Several empirical studies have demonstrated the applicability of blockchain based security across specific IoT application domains. In smart energy systems, blockchain has been shown to enhance peer to peer energy trading security while ensuring transparent meter data validation (Gupta, 2022; Rahman et al., 2022). In healthcare IoT, blockchain based access control mechanisms improve patient data integrity and auditability while reducing unauthorized access risks (Alam, 2020). Industrial IoT research highlights how blockchain strengthens machine to machine authentication, protects sensor data from tampering, and supports secure coordination within cyber physical production systems (Uddin et al., 2023). Supply chain IoT studies confirm that blockchain improves traceability, reduces fraud, and enhances real time verification of logistics data (Khan et al., 2021).

Despite these advances, prior studies predominantly focus on isolated sectoral implementations or technical protocol efficiency, such as latency reduction, lightweight consensus algorithms, and transaction throughput optimization. Comparative investigations that evaluate how blockchain security functions operate across industries with different regulatory demands, risk tolerances, and performance constraints remain limited. This gap restricts the generalization of existing findings and weakens the theoretical consolidation of blockchain as a universal IoT security infrastructure (Ali et al., 2021).

The integration of resource-based view theory further explains the strategic value of blockchain enabled security for organizations operating IoT systems. Secure, transparent, and trustworthy data infrastructures constitute intangible organizational resources that enhance competitive advantage by reducing operational risk and strengthening stakeholder confidence. Blockchain based IoT security thus functions not only as a technical safeguard but also as a strategic asset that supports long-term digital resilience and ecosystem collaboration (Makhdoom et al. 2021).

Collectively, these theoretical foundations and prior empirical insights establish a strong analytical basis for examining blockchain as a cross industry IoT security mechanism. The accumulated evidence implicitly indicates that blockchain adoption strengthens data integrity, decentralizes trust, and enhances system resilience across heterogeneous IoT environments. At the same time, the sector-dependent differences observed in prior studies suggest that blockchain's security impact is shaped by contextual factors such as regulatory frameworks, system scale, and performance sensitivity. This theoretical synthesis provides the conceptual grounding for analyzing how blockchain secures IoT ecosystems across multiple industries within a unified analytical framework.

3. RESEARCH METHODS

This study adopts a cross-industry quantitative research design with a comparative explanatory approach to examine the role of blockchain in securing Internet of Things (IoT) ecosystems across multiple industrial sectors. The research design is structured to analyze the relationship between blockchain based security mechanisms and the perceived level of IoT security performance in different industries, including manufacturing, healthcare, energy, logistics, and smart infrastructure. The comparative design enables the identification of both convergent security patterns and sector-specific variations in blockchain adoption.

The population of this study consists of organizations that actively implement IoT systems integrated with blockchain technology across the selected industries. The research sample is determined using a purposive sampling technique, focusing on technology managers, cybersecurity specialists, system architects, and operational decision-makers who possess direct knowledge of IoT security implementation within their respective organizations. The final sample size fulfills the minimum requirements for multivariate statistical analysis to ensure adequate statistical power and generalizability of the findings.

Data are collected through a structured questionnaire distributed electronically to respondents across the targeted industries. The instrument measures key constructs including blockchain security capability, IoT data integrity, access control effectiveness, system resilience, and organizational trust in digital infrastructure. Each construct is operationalized into multiple indicator items using a Likert scale measurement. The validity and reliability of the instrument have been statistically tested, and the results indicate that all measurement items meet the acceptable thresholds for construct validity and internal consistency, confirming that the instrument is appropriate for further analysis.

The data analysis employs descriptive statistics and inferential analysis using multiple regression techniques to examine the influence of blockchain based security on IoT ecosystem protection across industries. The research model positions blockchain based security as the independent variable, IoT ecosystem security performance as the dependent variable, and industry type as a moderating variable. In this model, blockchain based security represents the extent to which decentralized ledgers, cryptographic authentication, and consensus mechanisms are applied in IoT operations. IoT ecosystem security performance reflects the level of data integrity, protection against cyber threats, and system reliability. Industry type functions as a contextual factor that influences the strength of the relationship between blockchain adoption and IoT security outcomes.

4. RESULTS AND DISCUSSION

Data collection in this study was conducted through a cross industry survey over a three-month period involving organizations that actively implement blockchain integrated Internet of Things (IoT) systems. The research locations covered multiple industrial zones representing the manufacturing, healthcare, energy, logistics, and smart infrastructure sectors. The collected data were processed using statistical analysis to examine the influence of blockchain based security mechanisms on IoT ecosystem protection. The results reveal a consistent positive relationship between blockchain adoption and improvements in data integrity, access control, and system resilience across all observed industries. Variations in effect strength emerge among sectors, reflecting differences in regulatory pressure, operational risk exposure, and system complexity. The findings are then interpreted by linking empirical outcomes with the core theoretical foundations of distributed systems, trust mechanisms, and information security governance. This section also compares the results with relevant prior studies to identify convergence and divergence patterns, while highlighting both theoretical contributions and practical implications for secure IoT deployment across heterogeneous industrial environments.

Data Collection and Study Context

Data collection for this study was carried out through a structured cross industry survey over a three month period, from March to May 2025. The survey targeted organizations that actively implement Internet of Things (IoT) systems integrated with blockchain based security mechanisms. Data were collected using an online questionnaire distributed directly to professionals responsible for digital infrastructure, cybersecurity, and system operations within their respective organizations. This approach ensured that the information obtained reflected actual implementation practices rather than theoretical perceptions.

The study context represents a multi sector industrial environment covering manufacturing, healthcare, energy, logistics, and smart infrastructure. These sectors were selected because they exhibit high levels of IoT dependency and significant exposure to cybersecurity risks. Manufacturing and logistics sectors rely heavily on real time sensor data and machine to machine communication, healthcare systems demand strict data integrity and access control, while the energy and smart infrastructure sectors depend on continuous system availability and resilience. The inclusion of these diverse industries enables a comprehensive cross industry analysis of blockchain enabled IoT security performance.

Respondents were selected using purposive sampling, focusing on individuals with direct involvement in IoT operation and digital security decision making. This included IT managers, system architects, cybersecurity analysts, and operational technology supervisors. The data collection process yielded a sufficient number of valid responses for statistical analysis and cross industry comparison. This study context establishes a reliable empirical foundation for examining how blockchain based security mechanisms operate across heterogeneous IoT environments with different operational risks and regulatory pressures.

Table 1. Profile of Data Collection and Study Context

Aspect	Description
Research Period	March – May 2025
Data Collection Method	Online structured questionnaire
Sampling Technique	Purposive sampling
Target Respondents	IT managers, system architects, cybersecurity analysts, IoT operators
Total Industry Coverage	Five sectors
Observed Industry Sectors	Manufacturing, Healthcare, Energy, Logistics, Smart Infrastructure
Focus of Data	Blockchain based IoT security implementation and performance

Source: Processed research data (2025)

Table 1 presents the profile of the data collection process and the study context. The research was conducted over a three month period using an online structured questionnaire and purposive sampling. Respondents consisted of professionals directly involved in IoT and cybersecurity operations across five industrial sectors. This table confirms that the data were obtained from relevant technical decision makers and represent diverse high risk IoT environments.

Descriptive Results of Blockchain Based IoT Security

The descriptive analysis of the research data provides an overview of how blockchain based security mechanisms are implemented within IoT ecosystems across the observed industries. The results indicate that the overall level of blockchain adoption for IoT security falls within the high category, reflecting a growing awareness of the importance of decentralized security architectures. Most participating organizations reported the active use of distributed ledger systems to record IoT transactions and device interactions, particularly for applications involving sensitive operational and transactional data.

In terms of cryptographic authentication, the findings show that blockchain is widely utilized to strengthen device identity management and prevent unauthorized access. Respondents from the manufacturing and healthcare sectors reported the most intensive use of cryptographic verification for IoT devices, driven by the need to protect production systems and sensitive patient data. Access control mechanisms based on smart contracts were also commonly implemented, enabling automated authorization processes that reduce human intervention and potential security breaches.

The descriptive results further reveal that system resilience is one of the most prominent benefits perceived from blockchain integration. Organizations in the energy and smart infrastructure sectors reported improved fault tolerance and reduced vulnerability to single points of failure due to the decentralized nature of blockchain networks. Meanwhile, the logistics sector emphasized the role of blockchain in enhancing data traceability and real time verification of asset movements across interconnected IoT devices.

Table 2. Descriptive Overview of Blockchain Based IoT Security Implementation

Security Dimension	Manufacturing	Healthcare	Energy	Logistics	Smart Infrastructure
Distributed Ledger Utilization	High	High	Moderate	High	Moderate
Cryptographic Device Authentication	High	Very High	High	Moderate	High
Smart Contract–Based Access Control	High	Very High	Moderate	High	Moderate
Data Integrity Protection	Very High	Very High	High	High	High
System Resilience and Fault Tolerance	High	Moderate	Very High	Moderate	Very High

Source: Processed research data (2025)

Table 2 summarizes the descriptive overview of blockchain based IoT security implementation across industries. The results indicate that manufacturing and healthcare show the highest levels of blockchain utilization for data integrity, device authentication, and access control. The energy and smart infrastructure sectors demonstrate the strongest performance in system resilience and fault tolerance. Meanwhile, the logistics sector emphasizes blockchain adoption for data traceability and transaction transparency. These patterns reflect sector specific security priorities within heterogeneous IoT ecosystems.

Cross Industry Comparison of IoT Security Performance

The cross-industry comparative analysis reveals that the impact of blockchain integration on IoT security performance varies across sectors, although a generally positive trend is observed in all industries. The manufacturing sector demonstrates a strong improvement in data integrity and machine authentication. The use of blockchain based ledgers ensures that sensor data and machine-generated information cannot be altered without detection, which enhances production reliability and minimizes the risk of cyber-induced operational disruptions. This sector also shows a high level of automation in access control through smart contracts, supporting secure machine-to-machine communication.

In the healthcare sector, the most significant improvement is observed in data integrity and access control effectiveness. Blockchain-enabled IoT systems provide immutable medical data records and strict authorization mechanisms, which are essential for protecting sensitive patient information. The comparative findings indicate that the security gains in healthcare are driven primarily by regulatory compliance requirements and the critical nature of medical data confidentiality.

The energy and smart infrastructure sectors exhibit the strongest performance in terms of system resilience and availability. Blockchain contributes to enhanced fault tolerance by distributing control across multiple nodes, reducing the risk of large scale service disruption caused by single points of failure. These sectors benefit from the high level of redundancy and transparency enabled by decentralized consensus mechanisms. In contrast, the logistics sector shows its most prominent gains in data traceability and transaction transparency. Blockchain-based IoT systems enable real-time verification of goods movement and asset status across supply chain networks. This capability significantly reduces the risk of data manipulation and fraud, while also improving coordination among multiple stakeholders.

Hypothesis Testing and Effect Analysis

The hypothesis testing results confirm that blockchain based security mechanisms have a statistically significant effect on the security performance of IoT ecosystems across industries. The inferential analysis shows that blockchain adoption positively influences key security dimensions, including data integrity, access control effectiveness, and system resilience. The partial effect testing indicates that each dimension of blockchain security contributes meaningfully to strengthening IoT protection, demonstrating that decentralized validation, cryptographic authentication, and automated authorization are not merely supportive features but core drivers of IoT security enhancement.

The simultaneous effect analysis further reinforces these findings by showing that the combined application of blockchain mechanisms produces a stronger impact on overall IoT security performance than any single mechanism operating independently. This result highlights the systemic nature of blockchain-based security, where integrity, transparency, and decentralization function as an integrated protection framework.

The analysis also reveals the moderating role of industry type in shaping the strength of the relationship between blockchain adoption and IoT security outcomes. Industries with high regulatory pressure and critical operational risks, such as healthcare and energy, exhibit stronger effect magnitudes compared with sectors characterized by lower compliance intensity. This indicates that contextual industry factors amplify the strategic value of blockchain based security.

Theoretical Interpretation of the Findings

The empirical findings of this study can be coherently explained through several theoretical perspectives that form the foundation of blockchain enabled IoT security. From the viewpoint of distributed systems theory, the positive impact of blockchain on system resilience and fault tolerance confirms the principle that decentralized control structures reduce the vulnerability associated with single points of failure. The improved availability and operational continuity observed particularly in the energy and smart infrastructure sectors are consistent with the theoretical expectation that distributed consensus enhances system robustness under cyber threats.

In relation to information security theory, the results strongly support the role of blockchain in reinforcing the integrity and availability dimensions of the classical security triad. The significant improvement in data integrity across manufacturing and healthcare sectors reflects the effectiveness of immutable ledgers in preventing unauthorized data manipulation. Likewise, the enhanced availability achieved through decentralized validation mechanisms validates the assumption that blockchain architectures strengthen continuous access to trustworthy system resources in highly connected IoT environments.

From the perspective of digital trust theory, the findings indicate a structural shift in trust formation from centralized authorities toward algorithm based verification mechanisms. The widespread use of cryptographic authentication and smart contract driven access control demonstrates that trust among heterogeneous IoT actors is increasingly embedded in programmable logic rather than institutional guarantees. This transformation is particularly evident in cross-organizational environments such as logistics and supply chain networks.

5. CONCLUSION AND SUGGESTIONS

This study confirms that blockchain based security mechanisms play a significant role in strengthening the security performance of Internet of Things (IoT) ecosystems across multiple industries. The results demonstrate that blockchain adoption consistently enhances data integrity, access control effectiveness, and system resilience in manufacturing, healthcare, energy, logistics, and smart infrastructure sectors. The hypothesis testing results provide empirical evidence that blockchain integration exerts a positive and significant influence on IoT security performance, while the strength of this effect varies according to industry characteristics, regulatory pressure, and operational risk levels. This finding indicates that blockchain is not merely a technical supplement but functions as a strategic security infrastructure within heterogeneous IoT environments.

From a practical perspective, the findings suggest that organizations operating IoT systems should prioritize blockchain integration as part of their core cybersecurity strategy, particularly in sectors with high data sensitivity and critical infrastructure dependence. Policymakers and regulators are also encouraged to develop cross-sector security standards that accommodate blockchain based architectures to ensure interoperability, transparency, and regulatory compliance. However, this study is limited by its reliance on survey based perceptions and its focus on selected industrial sectors, which may constrain broader generalization. Future research is therefore recommended to incorporate longitudinal designs, objective security performance metrics, and deeper technical evaluations of blockchain-IoT integration across a wider range of industries and geographic regions to strengthen empirical robustness and enhance theoretical generalization.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to Universitas BSI, Margonda Campus, Depok, West Java, Indonesia and Universitas BSI, Kramat 98 Campus, Central Jakarta, Indonesia for providing academic support and research facilities that enabled the successful completion of this study. The authors also extend their appreciation to all respondents from various industrial sectors who generously shared their time, experience, and insights regarding the implementation of blockchain based IoT security systems. In addition, the authors acknowledge the valuable feedback and constructive comments from colleagues and peer reviewers that significantly contributed to the improvement of this manuscript. This article is an independent research output developed as a contribution to the advancement of knowledge in the fields of IoT security and blockchain technology.

REFERENCES

Alam, T. (2020). Blockchain-based big data analytics for smart healthcare. *Future Generation Computer Systems, 109*, 739–748. https://doi.org/10.1016/j.future.2020.04.021

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2021). Applications of blockchain in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 23*(1), 48–85. https://doi.org/10.1109/COMST.2020.3034324

Chen, R., Xu, L. D., Lu, Y., & Chen, H. (2021). Exploring the integration of blockchain and Internet of Things: A survey. *Journal of Network and Computer Applications, 179*, 102991. https://doi.org/10.1016/j.jnca.2020.102991

Dai, H., Zheng, Z., & Zhang, Y. (2021). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal, 8*(18), 14606–14629. https://doi.org/10.1109/JIOT.2021.3057008

Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., & Janicke, H. (2020). Security for 5G and IoT: A survey. *Computer Networks, 169*, 107053. https://doi.org/10.1016/j.comnet.2019.107053

Gupta, A., Sharma, G., & Nirmala, S. (2022). A blockchain-based secure framework for IoT in smart cities. *Journal of Information Security and Applications, 65*, 103046. https://doi.org/10.1016/j.jisa.2022.103046

Hannan, A., Arshad, J., & Azam, M. (2022). Blockchain-based access control model for secure IoT. *Computers & Security, 112*, 102511. https://doi.org/10.1016/j.cose.2021.102511

Khan, M. A., Salah, K., Jayaraman, R., & Omar, M. (2021). Blockchain and IoT-based food traceability for smart agriculture. *IEEE Access, 9*, 29470–29485. https://doi.org/10.1109/ACCESS.2021.3057508

Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizani, M. (2020). BPDS: A blockchain-based privacy-preserving data sharing for electronic medical records. *IEEE Transactions on Industrial Informatics, 16*(3), 1783–1793. https://doi.org/10.1109/TII.2019.2948180

Makhdoom, I., Abolhasan, M., Ni, W., & Zhang, Y. (2021). Blockchain's adoption in IoT: The challenges and a way forward. *Journal of Network and Computer Applications, 176*, 102935. https://doi.org/10.1016/j.jnca.2020.102935

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). Blockchain for secure EHRs sharing of mobile cloud based e-health systems. *IEEE Access, 9*, 66792–66806. https://doi.org/10.1109/ACCESS.2021.3076717

Novo, O. (2020). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal, 7*(10), 8101–8113. https://doi.org/10.1109/JIOT.2020.2992584

Rahman, M. A., Hossain, M. S., & Alrajeh, N. A. (2022). Secure blockchain-based IoT architecture for smart cities. *Future Generation Computer Systems, 127*, 33–45. https://doi.org/10.1016/j.future.2021.08.044

Sharma, S., & Sood, S. K. (2022). Blockchain-based solutions to mitigate DDoS attacks in IoT. *Computers & Security, 115*, 102600. https://doi.org/10.1016/j.cose.2022.102600

Singh, S. K., Rathore, S., & Park, J. H. (2021). Blockchain-based privacy-preserving security framework for IoT-driven smart cities. *Sustainable Cities and Society, 69*, 102798. https://doi.org/10.1016/j.scs.2021.102798

Tang, J., Xie, S., & Yang, J. (2021). Secure data provenance in IoT environments using blockchain. *Sensors, 21*(7), 2334. https://doi.org/10.3390/s21072334

Uddin, M., Al Hameed, A., & Islam, M. (2023). Blockchain-enabled security framework for industrial IoT. *IEEE Transactions on Industrial Informatics, 19*(4), 5031–5042. https://doi.org/10.1109/TII.2022.3189654

Xu, J., Wang, K., Pei, L., Guo, S., Guo, M., Ji, Y., & Cai, H. (2020). A blockchain-based privacy preserving data sharing system for IoT. *IEEE Transactions on Parallel and Distributed Systems, 31*(6), 1329–1343. https://doi.org/10.1109/TPDS.2019.2955901

Yang, K., Ren, J., Zhu, Y., & Zhang, W. (2022). Blockchain-based trusted data sharing among IoT devices. *IEEE Internet of Things Journal, 9*(5), 3562–3575. https://doi.org/10.1109/JIOT.2021.3097726

Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M. M., & Alamri, A. (2020). Health-care as a service: The role of cloud, IoT, and blockchain. *IEEE Access, 8*, 179096–179105. https://doi.org/10.1109/ACCESS.2020.3026852