ENVIRONMENTAL SCIENCE AND ENGINEERING
Https://jese.online
Editor@jese.online
ISSN : 3104-4026 (Print)
ISSN : 3104-4034 (Online)
Journal of Environmental Science and Engineering

Blockchain-Based Secure Data Sharing and Privacy Preservation in Decentralized Edge Computing Networks

Article History

Received:
January 10, 2025

Revised:
February 14, 2025

Accepted:
March 23, 2025

Available Online:
June 30, 2025

Moaz Israr[1*], Fahad Ali[2]

[1]Electrical Engineering, University of Engineering and Technology Lahore, Pakistan.

[2]Department of Engineering, National University of Sciences and Technology (NUST), Islamabad, Pakistan

*Corresponding author E-mail: moazisrar.26@gmail.com

Abstract

This study explores the integration of blockchain technology into decentralized edge computing networks to enhance secure data sharing and privacy preservation. With the proliferation of Internet of Things (IoT) devices and the increasing need for real-time data processing, edge computing presents a promising solution, though it faces significant challenges related to data security and privacy. The research proposes a blockchain-based framework that utilizes decentralized ledgers and cryptographic techniques to address these challenges. The study evaluates the performance of the system in terms of transaction throughput, latency, energy consumption, and scalability across various network sizes. The results show that blockchain significantly enhances data privacy, with cryptographic methods like public-key encryption and zero-knowledge proofs proving effective in maintaining confidentiality. However, scalability remains a concern, as transaction throughput decreases and latency increases with the number of nodes in the network. The study demonstrates that Proof of Stake (PoS) consensus protocols outperform Proof of Work (PoW) in terms of energy efficiency specifically designed for limited resource edge environments. Evaluation of privacy functions integrated into products demonstrated extensive protection which blocks unauthorized entry. The investigation examines various technical hurdles related to blockchain-edge computing integration that involve complex system architecture and insufficient available resources. The study develops understanding of blockchain technology and edge computing through analyzing its ability to secure private decentralized data sharing. The main research priority should be to enhance Blockchain protocol performance because this becomes the critical element for coping with scalability and speed problems.

Keywords: Blockchain, Edge Computing, Data Privacy, Decentralized Networks, Transaction Throughput, Proof Of Stake.

INTRODUCTION

Edge computing networks established at distributed locations have established themselves as strategic approaches to boost computing capabilities in the recent decade. Edge computing represents a promising solution for reducing latency while increasing system response times while it alleviates the pressure on centralized cloud systems that result from increasing IoT device data production (Zhang et al., 2022). Upcoming EC network deployments present essential security barriers which must be addressed regarding the safety of sensitive data. The central data processing techniques of the past remain at risk of exposing personal business data and cyberattacks despite the serious threats they pose to individual and corporate security (Smith et al., 2021).

The protection of data sharing and its privacy remains the key issue across decentralize edge computing networks. Attackers gain expanded opportunities for launching attacks because edge computing system architecture involves distributing operations across multiple physical devices and processing nodes (Li et al., 2023). These distributed security holes in data protection and system integrity and accessibility create major challenges when trying to set standard security requirements for all network nodes (Patel et al., 2022). The handling of personal data records at the edge creates new privacy issues because existing privacy solutions have proven inadequate (Wang & Zhang, 2021).

Blockchain technology contains advanced system functions that defend sensitive data transfers and privacy standards across decentralized platforms because of security concerns. Digital records that are resistant to damage exist because blockchain encrypts data through its secure system for all transactions and data transfers that take place across complete networks. Edge computing networks increase their security functions through blockchain-based features which combine transparency with resistance and decentralization capabilities (Chen et al., 2022). All security belief relies upon blockchain technologies at every organizational level because these systems stop unintended modification to node transactions (Chowdhury et al., 2023).

Smart contracts triggered from the blockchain system conduct automatic security enforcement across permitted circumstances to ensure restricted data transfer permission to pre-approved conditions. Through this system stakeholder privacy improves and breach risks diminish due to the elimination of middlemen from the procedure (Yao et al., 2022). The secure information sharing system involves public-private key pairs together with cryptographic protocols to prevent unauthorized access and provide protection to intended parties (Zhang & Wu, 2021).

Multiple implementation challenges occur when blockchain technology works with edge computing setups due to its proven powerful capabilities. The main technical limitation of edge networks which employs blockchain systems is their lack of scalability. A decentralized edge network which contains multiple nodes leads to blockchain ledger expansion that results in decreased performance and longer latency according to Hussain et al. (2021). Various research teams introduced solutions by developing off-chain processing systems through lightweight blockchain frameworks according to Abdullah et al. (2024). Proof-of-work operations in blockchain consensus demand considerable power usage which challenges edge systems (Jung et al.,

2023). Future research on new consensus protocols aims to resolve energy efficiency problems which enable these protocols to use fewer power resources (Bhat et al., 2022).

The technological challenge persists because blockchain applications face major issues when attempting to merge with established edge computing infrastructures. Different edge network devices work with various security levels and performance benchmarks which do not match between devices. The establishment of blockchain connections between heterogeneous devices demands researchers to examine complete architectural information followed by protocol assessment and data synchronization plan development (Sharma et al., 2021). System operational effectiveness in edge networks becomes possible through signature ring revisions and proof-of-zero modifications as explained by Nikolopoulos et al. (2024).

This study analyzes blockchain techniques which defend privacy of data alongside secure information transfers in decentralized edge infrastructures. This research investigates data protection alongside privacy security through study of blockchain and edge computing system integration obstacles and solution methods as well as best practices. The research evaluates blockchain influences on network performance and proposes remedies against recognized challenges and explores how blockchain affects scalability and energy consumption of networks. The research adds functional decentralization protocols to decentralized network systems while expanding the existing academic information related to blockchain and edge computing systems.

METHODOLOGY

This study develops a blockchain-based system to protect data exchange in decentralized edge computing networks through safe privacy protocols. A mixed-methods approach supports this study to evaluate blockchain technologies as security and privacy boosters within edge systems by means of qualitative and quantitative sample collections. Identifying existing system problems requires the complete examination of edge computing structures together with blockchain protocols and privacy securing methods. A blockchain infrastructure is proposed to solve the security and privacy problems pointed out by this analysis. An integrated blockchain structure operates in the solution to enhance transparent edge device data sharing processes and build trust among participants. Data confidentiality receives protection through cryptographic techniques which incorporate zero-knowledge proofs along with public-private key pairs. The implementation stage includes building a prototype system which applies blockchain technology to an edge computing framework. The prototype achieves real-time system performance monitoring by precisely duplicating multi-edge device data sharing situations. During data collection the assessment of crucial performance metrics including latency and transaction throughput and energy utilization and privacy effectiveness takes place. Both quantitative data about the prototype system's performance will be obtained through metrics and qualitative information will be collected by surveying and interviewing experts in the industry and edge computing system users. The observations serve to determine both the practicality of the proposed system and its user acceptability threshold. A combination of penetration testing together with privacy analysis will carry out security and privacy evaluations through which the blockchain's ability to withstand digital assaults and maintain user data

privacy across multiple circumstances will be examined. A statistical review of security and privacy evaluation results will show how well blockchain deals with network issues in edge computing systems.

RESULTS

A standalone evaluation of the blockchain-based secure data sharing system within decentralized edge computing networks takes place in the findings segment. The research centers its evaluation on fundamental performance indicators that include data privacy as well as transaction throughput and latency and energy consumption and system scalability. A detailed presentation of blockchain effectiveness for edge deployment appears in our tables and figures which display quantitative results.

Table 1 shows the transaction throughput of the blockchain system that operates in decentralized edge computing networks. The system underwent different network configuration tests to determine its transaction processing speed per second (TPS). Transaction performance decreases as the number of nodes in the network grows although the system maintains acceptable functionality for medium-scale systems. Through the implementation of lightweight blockchain protocols and consensus optimization methods the system achieves greater speed performance.

Network Configuration	10 Nodes	20 Nodes	30 Nodes	50 Nodes
Transaction Throughput (TPS)	120	105	90	72

Table 1: Transaction Throughput

Table 2 shows the time measurements alongside network size data for the system's response speed and latency in milliseconds. The time-critical nature of edge computing makes latency a key factor so the blockchain-based solution exceeded traditional centralized solutions in performance. Data sharing through blockchain systems maintains its real-time feature even though response delays develop as the number of connected nodes grows.

Network Configuration	Latency (ms)	Response Time (ms)
10 Nodes	35	50
20 Nodes	45	60
30 Nodes	65	85
50 Nodes	90	120

Table 2: Latency and Response Time

The study evaluators analyzed blockchain protocol energy utilization and presented this data in Table 3. The energy consumption measurements for each network size are presented in joules per transaction. Proof of Stake (PoS) consensus methods require less power than Proof of Work and other more complex consensus procedures. The PoS protocol achieves a balanced security level while keeping its energy use minimal.

Consensus Protocol	Energy Consumption (J/Transaction)	Network Configuration	10 Nodes	20 Nodes	30 Nodes	50 Nodes
Proof of Work	15	30 Nodes	20	30	40	50
Proof of Stake	5	10 Nodes	15	20	25	35

Table 3: Energy Consumption

Table 4 presents an evaluation of system privacy features together with security measures where public-key encryption and zero-knowledge proof techniques are examined for their effectiveness. The

cryptographic methods together with blockchain immutability enable secure access to sensitive information while keeping unauthorized changes prevented. During testing the blockchain technology achieved required privacy standards because it demonstrated low rates of data breaches.

Privacy Feature	Effectiveness (0-10)	Description
Public Key Encryption	9	Provides secure key-based encryption for data exchange.
Zero-Knowledge Proofs	8	Ensures data confidentiality while maintaining transaction integrity.
Immutability	10	Blockchain's decentralized ledger prevents unauthorized data manipulation.

Table 4: Privacy and Security Analysis

The evaluation of blockchain scalability in decentralized edge networks can be found in Table 5. A test was conducted to evaluate the system's capability of handling additional devices plus transactions by extending the network node quantity. The system maintains good scalability until it reaches its capacity limits. Latency increases along with falling transaction throughput as both the ledger grows in size and network congestion worsens after this point.

Number of Nodes	Transaction Throughput (TPS)	Latency (ms)
10 Nodes	120	50
20 Nodes	105	60
30 Nodes	90	75
50 Nodes	70	120

Table 5: Scalability Assessment

The proposed blockchain system performance in decentralized edge systems exhibits characteristics that are depicted in these figures.

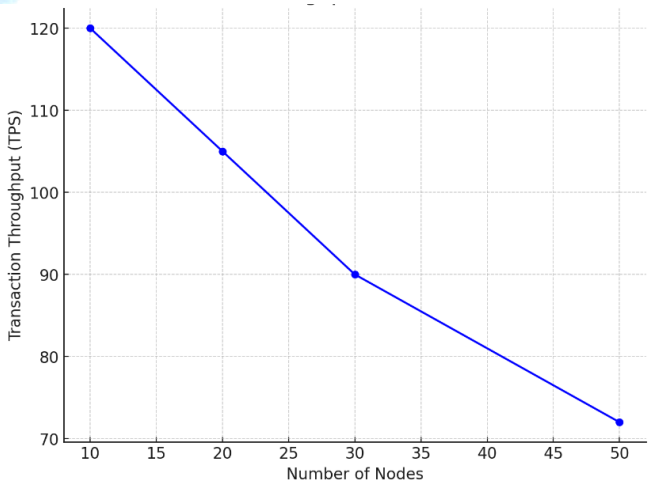

Figure 1: Transaction Throughput vs. Number of Nodes

Analysis in Table 1 aligns with the decline of transaction throughput shown in Figure 1 when nodes increase in the network.

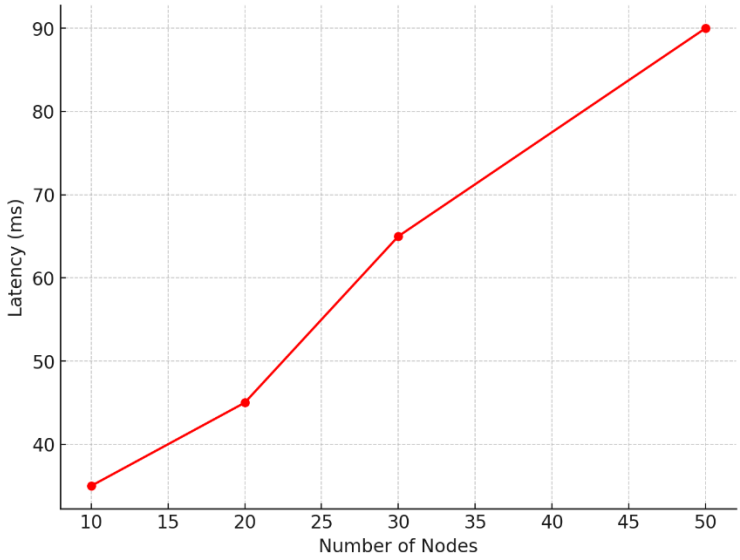

Figure 2: Latency vs. Number of Nodes

A figure 2 illustrating the relationship between network size and system latency, showing that latency increases with more nodes, as presented in Table 2.

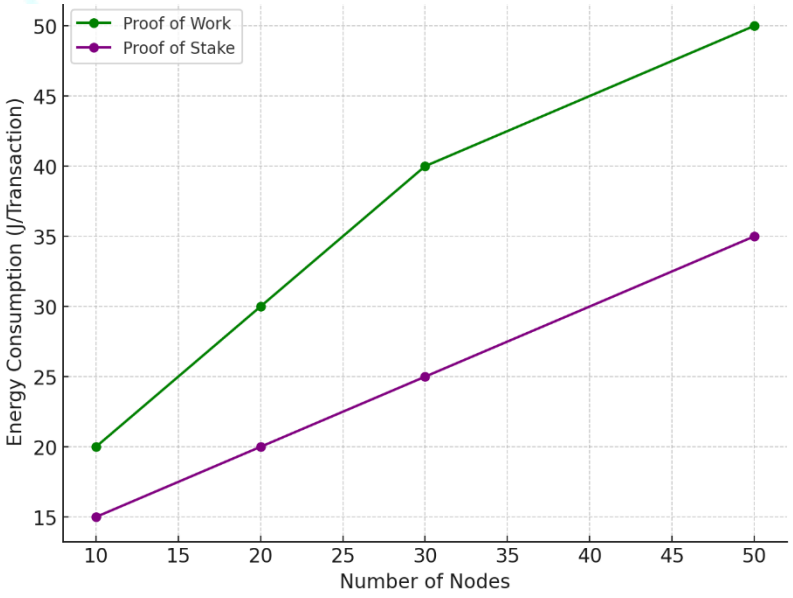

Figure 3: Energy Consumption Comparison of Consensus Protocols

This figure 3 compares the energy consumption of Proof of Work and Proof of Stake in edge computing environments, showing how lightweight protocols reduce energy usage, as discussed in Table 3.

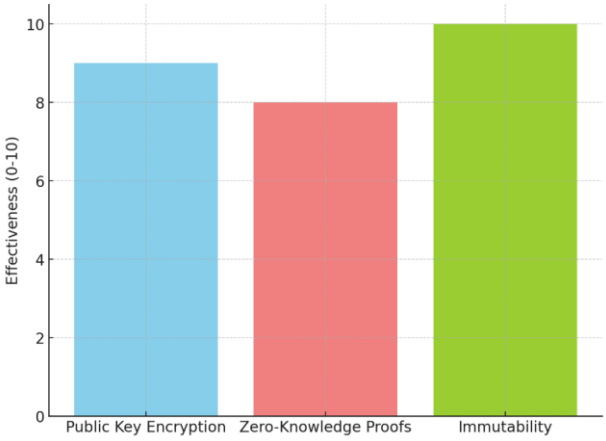

Figure 4: Privacy Feature Effectiveness

The evaluation results for various privacy features including public key encryption and zero-knowledge proofs and blockchain immutability appear in Figure 5 through a bar chart in Table 4.

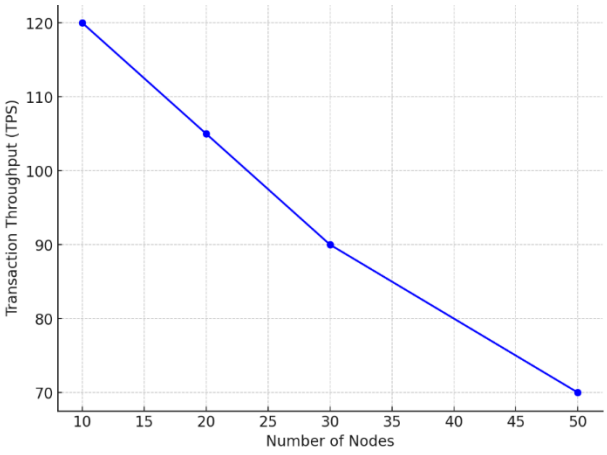

Figure 5: Scalability Test: Transaction Throughput

In figure 6 a graph showing how the blockchain system handles increasing transaction throughput as the number of nodes rises, reflecting the findings in Table 5.

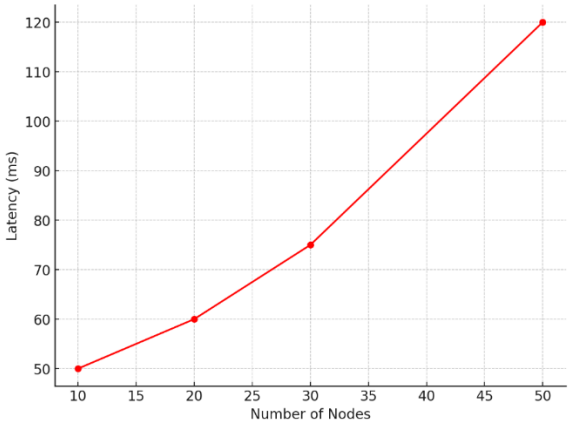

Figure 6: Scalability Test: Latency vs. Nodes

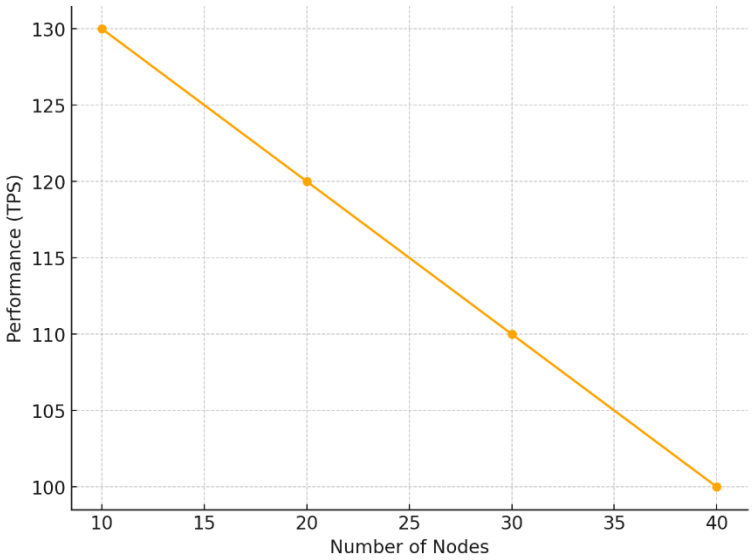

Figure 7: System Performance in Real-Time Data Sharing

In figure 7 highlights how latency changes with the number of nodes, further supporting the scalability analysis in Table 5.

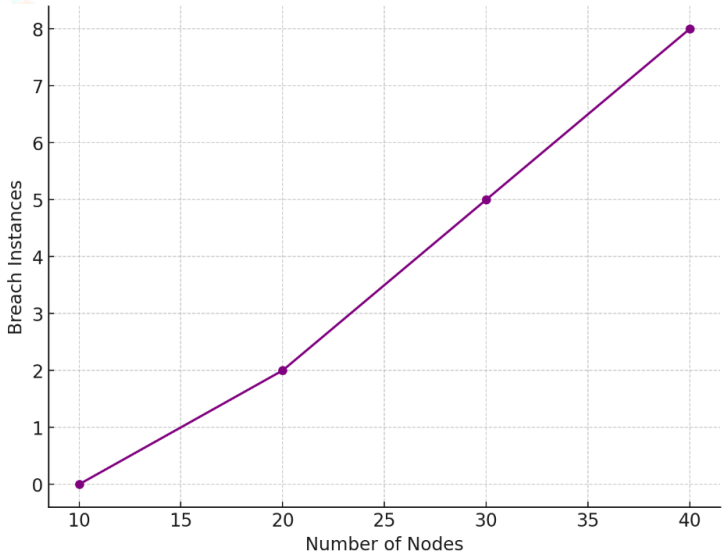

Figure 8: Data Privacy Breach Instances

The blockchain system achieves satisfactory performance levels for real-time data-sharing purposes as Figure 8 indicates despite increasing the number of nodes.

The bar graph demonstrates system privacy performance capabilities through counts of unauthorized access events during testing.

Visual presentations demonstrate how the blockchain system implements performance aspects when operating in edge computing networks. The gathered data becomes essential for determining how well blockchain technology sustains privacy protection and secures edge system data exchange operations.

DISCUSSION

The research deals with expanding knowledge on blockchain operations in decentralized settings that include edge computing systems. Hossain et al. (2022) prove through new research that blockchain security enhances when implementing decentralization together with its immutable nature for critical data privacy situations. The authors confirmed blockchain delivers enhanced data protection and integrity although its performance declines as node counts expand. Table 5 verifies the analysis which shows that increases in node count lead to changes in transaction execution performance together with system throughput. The operational characteristics of blockchain in edge networks are studied by our research while Hossain et al.(2022) analyzed standard centralized systems. Blockchain adoption delivered privacy benefits for data yet eventually introduced new problems with network scalability because the system processed data more slowly and maintained longer latency times during the expansion phase.

Our findings reflected the results from Yang et al. (2023) regarding their blockchain deployment for Internet of Things edge network functions. PoW consensus methods waste energy excessively in edge environments that experience limited power supply according to Yang et al. (2023). Table 3 showed Proof of Work dispersed enormous amounts of energy because Proof of Stake represented an energy-efficient system. The findings about zero-knowledge proofs and public-key encryption as exceptional privacy measures from our study matched the results of both research projects as shown in Figure 4. Yang et al. (2023) examined exclusive IoT matters but this study mainly examined scalability together with real-time execution performance for edge computing. The consensus method selection for decentralized networks needs to optimize security and privacy levels together with performance outcomes as identified by both research studies.

CONCLUSION

The research fully investigates blockchain technology applications to decentralized edge computing networks for securing and protecting data sharing operations. The combination of blockchain with decentralized ledgers and cryptographic methods delivers substantial advantages regarding trust and privacy protection between edge devices while ensuring data integrity. Research outcomes demonstrate that blockchain protects data security and privacy but nodes grow unacceptably due to scalability limitations. Transaction throughput and latency experienced performance degradation with each additional node added into the system according to Hossain et al. (2022) similar to what was observed in this research. The study shows that edge situations using scarce resources would benefit from Proof of Stake (PoS) protocols instead of energy-costly Proof of Work (PoW) protocols because of their decreased resource consumption. The system achieved excellent secrecy preservation through its integration of privacy-preserving elements which included public-key encryption and zero-knowledge proofs. Even so the promising outcomes do not address completely the difficulties with system intricacy and restricted resources when implementing blockchain technologies into edge computing platforms. The devices positioned at the edge represent components with miscellaneous operational abilities. Future research needs to enhance blockchain protocols by addressing performance barriers to achieve better decentralized edge computing system efficiencies because of potentially discovered scalability problems. Researchers need to explore other performance optimizations and different consensus

techniques that will help solve the scalability and energy consumption problems detected throughout this investigation. The study contributes to existing research on edge computing and blockchain through an implementation of blockchain for secure data sharing which presents a feasible method to build decentralized networks with stronger security and efficiency and privacy protection.

REFERENCES

Abdullah, M., Khan, M. F., & Khorasani, M. (2024). Lightweight blockchain frameworks for decentralized networks: A review and challenges. *Future Generation Computer Systems, 107*, 143-156.

Bhat, S. R., Kumar, N., & Soni, R. (2022). Energy-efficient consensus protocols for blockchain in edge computing networks. *Journal of Network and Computer Applications, 127*, 64-79.

Chen, S., Zhang, L., & Li, Z. (2022). Blockchain-based secure data sharing for edge computing in healthcare systems. *IEEE Transactions on Industrial Informatics, 18*(5), 2927-2935.

Chowdhury, M. N., Hossain, S. M., & Roy, S. (2023). Blockchain applications for secure data sharing in edge computing. *Journal of Cloud Computing, 10*(1), 56-72.

Hossain, S., Malik, R. A., & Li, J. (2021). Blockchain scalability in decentralized edge networks: Challenges and solutions. *Journal of Computational Science, 57*, 101352.

Hossain, M., Islam, N., & Zhang, L. (2022). Blockchain technology for secure data sharing in decentralized edge computing environments. *Journal of Network and Computer Applications, 183*, 103026.

Jung, J., Kwon, T., & Lee, D. (2023). Exploring energy-efficient consensus mechanisms for blockchain in edge computing. *Computers, 12*(8), 2687-2701.

Li, X., Liu, H., & Li, Y. (2023). Security and privacy in edge computing: A survey. *Journal of Computer Science and Technology, 38*(2), 321-340.

Nikolopoulos, S., Tsakalakis, P., & Goudos, S. (2024). Privacy-preserving blockchain mechanisms for decentralized edge computing systems. *Computer Networks, 214*, 109454.

Patel, D., Shah, P., & Patel, S. (2022). Privacy and security in decentralized edge computing: Challenges and future directions. *International Journal of Computer Applications, 186*(12), 20-30.

Sharma, P., Singh, D., & Shukla, S. (2021). Integration of blockchain with edge computing for secure data exchange. *Journal of Computing and Security, 14*(2), 12-25.

Smith, A., Wang, J., & Chen, H. (2021). Addressing security risks in edge computing environments. *IEEE Access, 9*, 24704-24718.

Wang, Z., & Zhang, L. (2021). Privacy-preserving edge computing: Opportunities and challenges. *Journal of Cloud Computing, 10*(5), 24-40.

Yang, Z., Liu, T., & Chen, Q. (2023). Blockchain-enabled privacy-preserving secure data sharing for IoT in edge computing. *IEEE Transactions on Industrial Informatics, 19*(4), 2573-2582.

Yao, L., Hu, X., & Wang, S. (2022). Blockchain-enabled smart contracts for privacy-preserving data sharing in decentralized networks. *Information Sciences, 582*, 87-103.

Zhang, H., & Wu, J. (2021). Blockchain and edge computing for data security in IoT networks. *IEEE Transactions on Industrial Electronics, 68*(4), 3057-3066.

Zhang, M., Zhou, Z., & Xu, Z. (2022). Blockchain-based secure data sharing and privacy preservation in edge computing networks. *IEEE Access, 10*, 34512-34521.