STM JOURNALS

Journal of
Advanced Database
Management & Systems

ISSN: 2393-8730
Volume 12, Issue 1, 2025
January—April
DOI (Journal): 10.37591/JoADMS

https://journals.stmjournals.com/joadms

Research JoADMS

A Systematic Review on Blockchain Technology for Maintaining Data Security in Cloud Systems

Ponnada Naga Ramya[1], I. Ravi Prakash Reddy[2,*], Supreethi K.P.[3]

Abstract

Cloud is one of the fastest growing technologies that is widely adopted in different types of application systems such as healthcare, smart network, supply chain management, internet ofthings (IoT), and many others. However, it is more prone to the security threats due to the inclusion of different technologies. Blockchain technology is currently being used to safeguard cloud data security, which provides the features of decentralization, resilience to failure, and transparency. This paper examines the security risks associated with the cloud, then briefly introducing blockchain technology and its types to address current problems in cloud data security. The motivation of this review is to conducta comprehensive analysis on blockchain technology in cloud computing. Also, it aims to evaluate the existing research works that investigate the usage of blockchain-cloud integration. Moreover, this study examines the benefits and drawbacks of using traditional blockchain technologies for cloud data security. In addition, a detailed performance analysis is carried out using different measures for analyzing the major effects of using blockchain technology in cloud systems.

Keywords: Cloud computing, blockchain, distributed ledger, data storage, security, cryptography, privacy

INTRODUCTION

Cloud computing technology [1, 2] is extensively used in recent days due to its rapid development and growth. As a result, it suffers from numerous security issues like data leakage, information loss, blocked calculations and etc. Hence,it is more essential to safeguard the cloud by using an advanced security methodology. The major benefits of using cloud computing are reduced maintenance cost, automated control, better scalability, and flexible data accessibility [3]. Due to theirenormous benefits, most of the corporations have adopted the cloud technology for data storage and retrieval. However, the privacy and security issues may create some significant drawbacks in hampering the cloud. The typical cloud environmentsecurity model is shown in Figure 1. Blockchain technology [4] iscurrently being used to safeguard cloud security of information,which is a highly anticipated trend for the computing sector. The industries seeking advancements in security and privacy are turning towards blockchain technology. A distributed ledger called blockchain [5] stores the tamper-evident data in the formof chain without centralized source, where the nodes are considered as the components or users. Moreover, the blockchain enables a distributed system, where all network nodes can actively participate in the data validation and verification processes.

***Author for Correspondence**
I. Ravi Prakash Reddy
E-mail: irpreddy@gnits.ac.in

[1]Assistant Professor, Department of Information Technology, G. Narayanamma Institute of Technology and Science (For Women), Hyderabad, Telangana, India
[2]Professor, Department of Information Technology, G. Narayanamma Institute of Technology and Science (For Women), Hyderabad, Telangana, India
[3]Professor, Department of Computer Science and Engineering, JNTUH UCEST, Hyderabad, Telangana, India

Received Date: September 18, 2024
Accepted Date: November 29, 2024
Published Date: December 31, 2024

Citation: Ponnada Naga Ramya, I. Ravi Prakash Reddy, Supreethi K.P. A Systematic Review on Blockchain Technology for Maintaining Data Security in Cloud Systems. Journal of Advanced Database Management & Systems. 2025; 12(1): 31–39p.

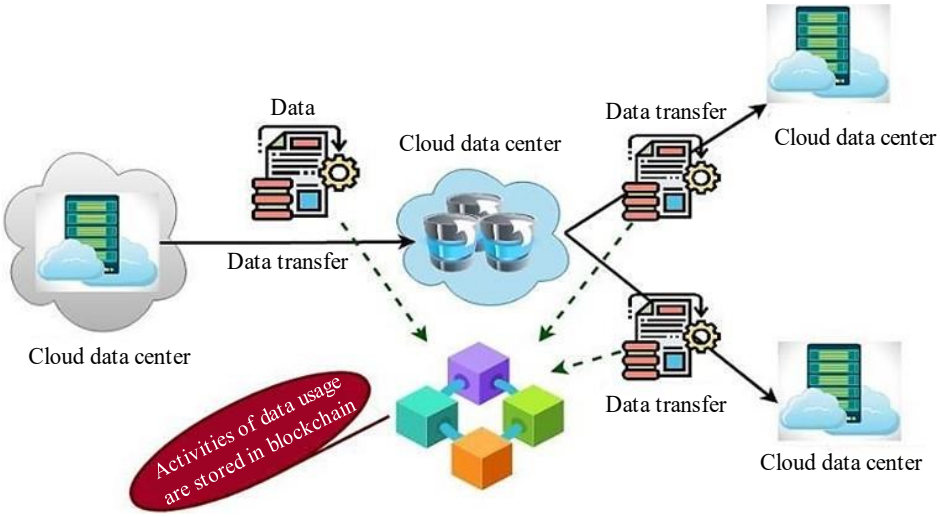

Figure 1. Architecture model of blockchain enabled cloud system.

In this technology, cryptography isused to encrypt the data that will be stored in the blockchain. Each block has a timestamp value, a secret hash, and a hash of the block before store it in the chain [6]. As a result, the blockchain records are tamper-proof, which eliminates the data privacy problems by an independent verification of participating individuals. By using this paradigm, a lot of privacy issues can be reduced with the security of information, availability of services, and effective cloud data management [7, 8]. Due to some of its features, such as data transparency and tamper-resistance, blockchain [9, 10] is considered to be a suitable choice for creating a trustworthy platform. There are a number of factors, such as legal constraints or administrative responsibilities that prevent the complete demise ofcentralization-based governance. According to the recent studies [11, 12], it is examined that the privacy leakage poses aserious threat to the blockchain-based autonomous trading system. Since the data are stored in the blockchain, it is accessibleto the general public. The goal of this survey is to emphasize recent developments in the blockchain integrated cloud storagemechanisms [13]. Moreover, the different types of technical features that affect blockchain are addressed, which include effectiveness, cost of energy, platform characteristics, and privacy. The objectives of this paper are given below:

- To provide a thorough analysis of blockchain technology in relation to cloud computing.
- To investigate the existing studies that exploring the use of blockchain-cloud integration.
- To examine the pros and cons of implementing the conventional blockchain techniques for cloud data security.
- To conduct a detailed comparative among therecent blockchain methods using a variety of performance and security measures.

The other portions of this paper are segregated into the following sections: The second section provides the complete literature review on the existing blockchain enabled cloud security models with their positives and negatives. Additionally, the third section conducts a thorough analysis of blockchain, including its unique features and applications. The fourth section demonstrates the effectiveness and outcomes of the traditional blockchain approaches employed in the cloud systems. The review is concluded in the final section along with its findings, observations, and future scope.

RELATED WORKS

Here, some of the recent blockchain techniques used in thecloud systems are reviewed with their pros and cons.

Privacy of information, high costs of operation, and data consistency are just a few problems this strategy raises [14]. The network nodes in the blockchain data storage scheme individually maintain

redundant data, which can be managed and controlled digitally without being altered by a single node [15]. Blockchain, or ledger technology, is an innovative technology scheme that consistently preserves and archives information by merging many technologies, taking into accountthe security concerns with the storage of decentralized data overnetworks [16]. The term "distributed" at this stage refers to the dispersal of both data storage and data gathering modes [17, 18]. In general, encryption of data files within a distributed ledger system guarantees privacy and security; however, it is essential to use present security sharing methods to address problems [19]. Blockchain technology is now being used in a number of ongoing studies in distributed storage systems for network data storage. To create unfamiliar encoded data, traditional encoding techniques need to reconstitute the originaldata [20, 21]. As a result, the blockchain-based networking storage system has to download enormous amounts of data whenever a particular node fails and rely on coding technologyto guarantee the accuracy of the network data [22]. Mahajan, et al. [23] utilized a new blockchain technology for protecting electronic health records stored in cloud systems. Here, the emergency of using blockchain technology is discussed by the authors for data security. Zuo et al. [24] implemented a Blockchain Ciphertext Attribute based Security (BCAS) for cloud systems. In comparison to previous storage models, this type of data exchange is more flexible and efficient. However, there are still a lot of issues with cloud storage security that have not been entirely resolved, like user authorization, authentication, and the data sharing securely. Data owners (DOs) in this system have the capacity to control who has access for decoding the data. The key is used to decode data must be negotiated between data requesters (DRs) and the DOs throughthe Business Communication Standards (BCS) [14, 25]. It is highly efficient in encryption and decryption, which could be the major benefit of this work. Kollu et al. [26] investigated the different types of blockchain techniques for securely storing data in cloud. The application ofblockchain technology to safeguard cloud computing is examined in this study. Typically, the blockchain [10, 27] is viewed as a proactive solution for present technology issues like decentralization, verification, and confidence even though it is still in its early phases of development. If the best method for storing and accessing cloud data is searched after, the innovative blockchain offers significant input. This study examines the potential of blockchain technology to secure cloud computing [28]. This study also offers a solution for secure data management in a cloud computing environment. This application uses electronic agreements, and authorization lists to protect user data. Khanna et al. [29] presented a comprehensive survey to examine the different types of blockchain methodologies for cloud security. Tabrez et al. [30] deployed a blockchain technology for avoiding security threatsin cloud system. Typically, the computer systems are vulnerable to cyberattacks. When configuring the information technology systems, the security of the database had to come first. The hackers mostly targeted the financial systems. Hence,the individual key address needed to be kept private and malware-free. The information could be instantly accessed from anywhere at any time due to cloud computing, which turned out to be the most adorable way to store data. In order toprevent information from being deduced, the protected database has to be carefully constructed and examined. Table 1 provides the comparative analysis among the existing access controllingmechanisms used in cloud systems.

METHODOLOGY

The decentralized cloud storage networks use the client side encryption, which is identical to the standard approach, formaintaining data security. The primary challenge associated with managing encrypted data is guaranteeing data usability. To put it more specifically, the owner of the data must be able to permit others to do searches on the remotely encoded dataset and get incomplete but valuable content [31]. The anonymous accessmanagement feature enables the data user to deceive the blockchain nodes for pretending that they possess a certificate issued by the data owner in an anonymous manner. As a result,the blockchain nodes only have knowledge that the user's permission has been granted by the data owner; they remain ignorant of the true identity of the data consumer or how often somebody has presented the credential authentication. An efficient method for a data consumer to locate the particular encrypted data is the secret keyword search [32]. The data user interfaces with blockchain nodes and blockchain material to obtain the fingerprint of the specific data contents according tothe search terms (or the qualities) instead of obtaining the wholeset of data. The encrypted documents are

subsequently obtainedby the data user from the decentralized offline storage of data. Typically, the data owners can outsource an extensive amount of data to the network via block data storage unit. In order to lessen the load on any particular node, the system fragments the data content and transmits its components among peer nodes. High availability is guaranteed by replicating and partitioning the data appropriately among the nodes [33].

As shown in Figure 1, blockchain breaks everything down into small chunks or blocks that are then broadcast to the entire network rather than being loaded into a cloud server or reservedfor a specific location.

Structure of Blockchain

Blockchain is a distributed ledger that securely stores data, in which the transaction is the fundamental unit of records. Blockchain technology could be leveraged to ensure access control for data gathered in a shady cloud environment [34]. The method is required in the untrusted cloud storage environment to safeguard shared data. Blockchain maintains an unaltered record of all important security-related actions, such as generating keys, privilege control selection, and revocation, using distributed blockchain systems. In order to mine the validated transactions into cryptographically protected blocks, nodes also known as block miners can verify the transactions by checking the signature that is linked to it. A widespread consensus problem must be resolved in order to permit a minerto generate a block [35]. The new blocks are distributed across the network by the miners who are successful in solving the consensus challenge. This happens after all transactions contained in the block have been verified and it has been verified that the block contains the solution to the consensus problem. By utilizing cryptographic techniques, the new block contains a connection to the previous block in the chains [36]. The blockchain-based cloud data storage system is shown in Figure 2. The use of smart contracts on the blockchain has the followingbenefits: making contracts hard to modify and lowering the costof delivery, verification, and identification of fraud. Blockchainoffers decentralized data storage with a secure ledger made up of blocks chained in sequence through multiple networks. It canuse cryptography to record and safeguard transactions or transactional events [37].

Characteristics of Blockchain

The blockchain verifies each transaction, and trustworthy miners record the transaction information. It is challenging to roll back or delete the transactions once they are on the list.

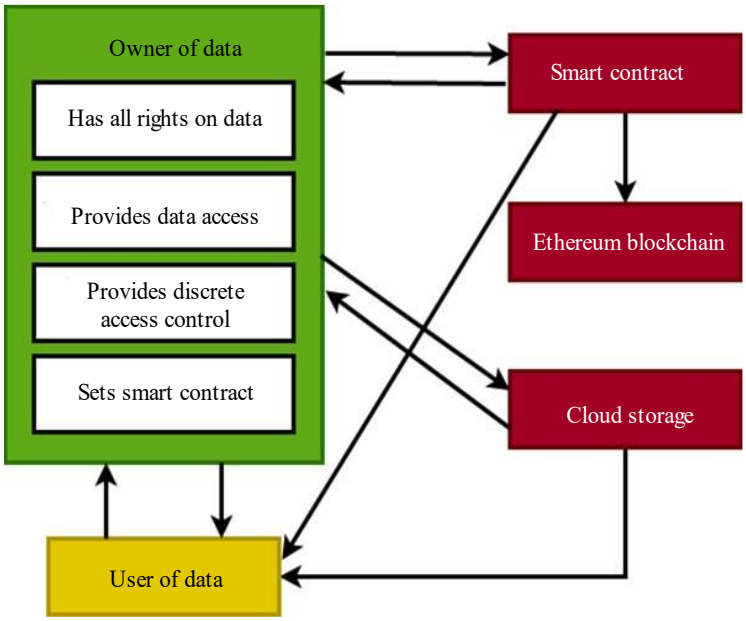

Figure 2. Blockchain-based cloud data storage system.

Additionally, the block verification can be performed by other miners, making them impenetrable to manipulation [38]. Data security in the blockchain is accomplished using the encryption models. Moreover, the blockchain technology provides security for information, verification, and validation. Data in blockchain is fully encrypted and digitally signed; it is also guaranteed not to be changed. Due to its assigned essence, users are able to verify that the data has not been altered or modified by looking at signatures at every log and ledger on every node in the network. When a signature does not match or is invalid during the verification process, an organization will quickly be made aware of any data manipulation by an attacker [39]. Blocks in blockchain technology are irreversible in nature, which means they cannot be changed. Since it can be challenging to address problems in a smart contract's records, hackers took advantage of this vulnerability to launch an attempt at stealing forks.

RESULTS AND DISCUSSION

This section validates the performance outcomes of using blockchain technology in the cloud data storage system. A framework that impacts blockchain technology has been provided in a number of research in order to provide safe distributed data storage and the provision of finding keywords [40]. For analyzing the major impacts of using blockchain technology, the different types of parameters such as energy consumption, block generation, and time consumption are validated in this study. Energy is used for transmitting, retrieving transactions, and verifying blocks on the replicated network. Figure 3 shows the energy consumption analysis with respect to the number of users in the cloud system [41]. The graph demonstrates that energy consumption proportionally rises as the number of users in the network increases since each user is responsible for validating a certain number of blocks. The visualization shows that the energy consumption was consistent with the number of servers within every group. Figure 4 shows the block generation time (in milliseconds) of the flat and vertical network architectures. Typically, the time needed for transmitting, creating blocks, and validating blocks is included in the block generation time.

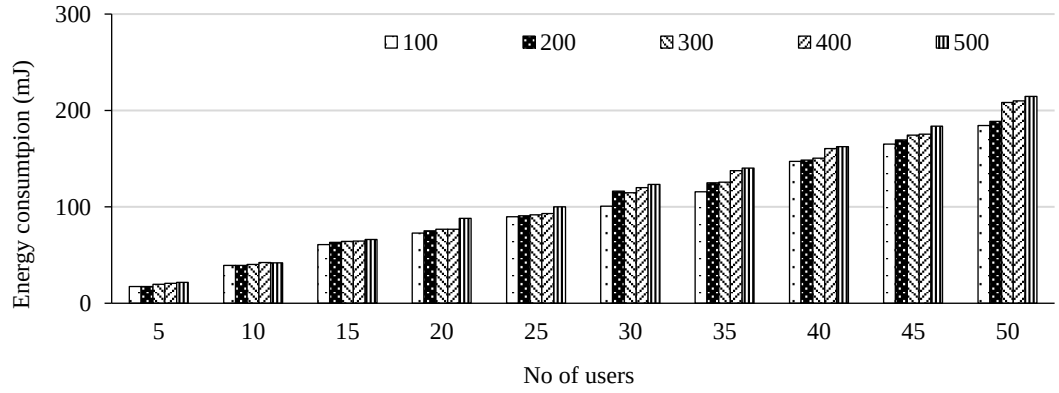

Figure 3. Energy consumption analysis.

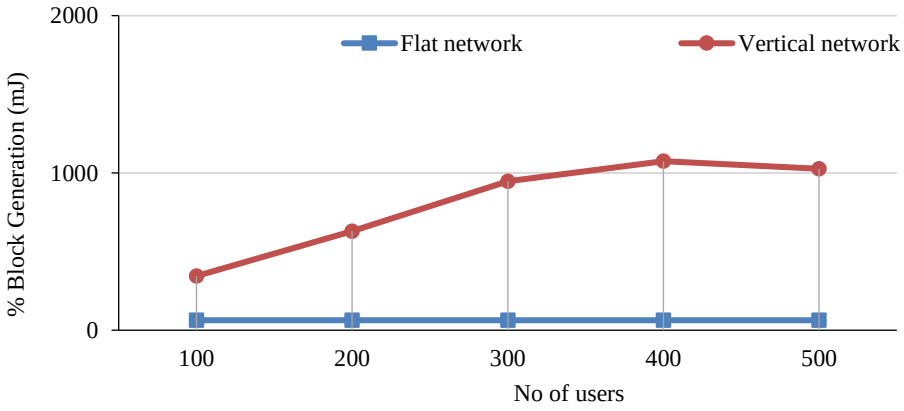

Figure 4. Block generation time

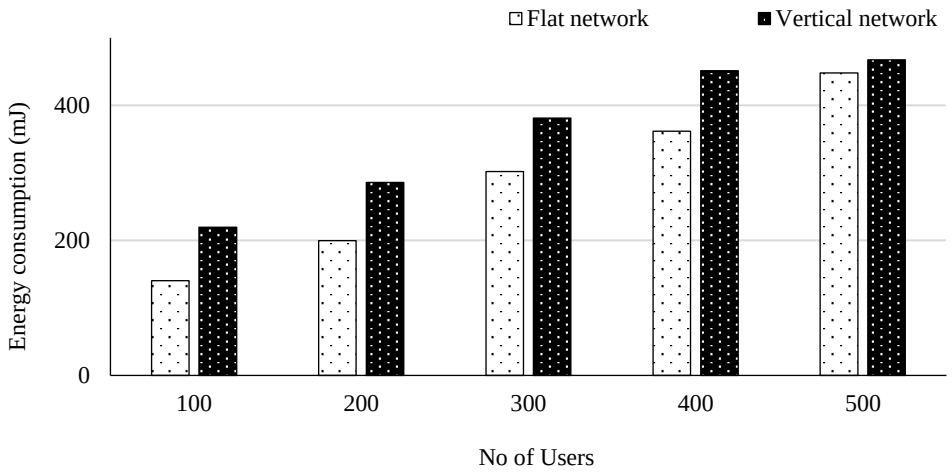

Figure 5. Energy consumption for flat and vertical networks.

Figure 5 shows the energy consumption analysis of the flat and vertical network architectures with respect to the number of users in the cloud systems. Overall, the results indicate that the energy consumption and time consumption both are increased with the increase of number of users in the cloud network. Table 1 presents the comparative analysis based on the security requirements of blockchain technology. In addition, Table 2 investigates the different types of blockchain integrated cloud data storage security models based on the different security properties.

Table 1. Comparative analysis based on security requirements.

Properties	Centralized	Decentralized	Data Chaining
Immutable	X	✓	+
Non-repudiation	X	✓	+
Integrity	X	✓	+
Transparency	X	✓	+
Equal rights	X	✓	+
Trust	X	✓	+

✓ More favorable, X - not positive, and + - most promising.

Table 2. Adoption of blockchain technology for cloud data storage.

Technique	Confidentiality	Integrity	Authentication	Access Control	Searching	Auditing	Distributed Data Storage
Blockchain with private key search	Yes	Yes	No	Yes	Yes	No	Yes
Blockchain – deduplication	Yes	Yes	No	No	No	Yes	No
Blockchain – data integrity	Yes	Yes	Yes	No	No	Yes	No
Data integrity verification	No	Yes	No	No	Yes	No	No
Blockchain multi-level scoring system	Yes	No	No	No	No	Yes	Yes
Blockchain based cloud storage	Yes	Yes	Yes	Yes	No	No	N
Access control system	Yes	No	Yes	Yes	No	No	No

Role-based access control smart contract	Yes	No	Yes	No	No	No	No
Cloud storage with access control framework	Yes	No	Yes	Yes	No	No	No
Public key encryption with keyword search	Yes	No	No	No	Yes	No	No
Data provenance	No	Yes	Yes	No	No	Yes	No
Blockchain based medical service framework	Yes	No	No	No	No	No	Yes
Tamper proofing blockchain	Yes	Yes	Yes	No	No	No	No
Fine grained access control blockchain	Yes	No	No	Yes	No	Yes	Yes
Public auditing scheme blockchain	Yes	No	No	No	Yes	No	No
Decentralized public auditing scheme	Yes	No	Yes	No	No	Yes	No

CONCLUSION

This paper analyzes various threats in the cloud environment before focusing on the usage of blockchain technology in data security. There are numerous schemes available right now for securing the privacy of cloud data, enabling cloud data traceability, and confirming the correctnessof cloud data. In general, the cloud is one of the well-known and adaptive technology, since it has been around for so long. Nevertheless, people still encounter challenges with smooth integration, information management, and other cloud computing issues. A developing technology called blockchain is renowned for its reliability and truthfulness, which are the key features that are impacting public opinion. Integrating blockchain with cloud computing offers numerous advantages in terms of usability, reliability, security, data capacity, and more. In this study, we provide a brief overview of cloud computing and blockchain technologies, discussing how the combination of a blockchain network with a scalable cloud environment can enhance user data management, security, and trust. Furthermore, the key benefits and challenges of blockchain enabled cloud systems are reviewed in this study. Then, the performance measures such as block generation time,and energy consumption are considered for demonstrating the effectiveness of using blockchain technology in cloud networks. In future, the present work can be enhanced further by implementing a lightweight blockchain-based security for secure data storage in cloud systems.

REFERENCES

1. Sharadqh AA, Hatamleh HA, Saloum SS, Alawneh TA. Hybrid chain: blockchain enabled framework for bi-level intrusion detection and graph-based mitigation for security provisioning in edge assisted IoT environment. IEEE Access. 2023; 11: 27433–27449.
2. Pal K. Security implications of IoT applications with cryptography and blockchain technology in healthcare digital twin design. In: Gaur L, Jhanjhi NZ, editors. Digital Twins and Healthcare: Trends, Techniques, and Challenges. Hershey, PA, USA: IGI Global; 2023. pp. 229–252.
3. Rathore NK, Khan Y, Kumar S, Singh P, Varma S. An evolutionary algorithmic framework cloud based evidence collection architecture. Multimedia Tools Appl. 2023; 82 (26): 39867–39895.
4. Wu H, Liu X, Ou W. A novel blockchain-MEC-based near-domain medical resource sharing model. In: Xu Y, Yan H, Teng H, Cai J, Li J, editors. Machine Learning for Cyber Security. ML4CS 2022. Cham, Switzerland: Springer Nature; 2022. pp. 40–56.

5. Selvarajan S, Srivastava G, Khadidos AO, Khadidos AO, Baza M, Alshehri A, Lin JC. An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. J Cloud Comput. 2023; 12 (1): 38.
6. Wenhua Z, Qamar F, Abdali TA, Hassan R, Jafri ST, Nguyen QN. Blockchain technology: security issues, healthcare applications, challenges and future trends. Electronics. 2023; 12 (3): 546.
7. Chennam KK, Muddana L, Aluvalu RK. Performance analysis of various encryption algorithms for usage in multistage encryption for securing data in cloud. In: 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, May 19–20, 2017. pp. 2030–2033.
8. Aluvalu R, Uma Maheswari V, Chennam KK, Shitharth S. Data security in cloud computing using Abe-based access control. In: Das SK, Samanta S, Dey N, Patel BS, Hassanien AE, editors. Architectural Wireless Networks Solutions and Security Issues. Singapore: Springer; 2021. pp. 47–61.
9. Pabitha P, Priya JC, Praveen R, Jagatheswari S. ModChain: a hybridized secure and scaling blockchain framework for IoT environment. Int J Inform Technol. 2023; 15 (3): 1741–1754.
10. Aluvalu R, VN SK, Thirumalaisamy M, Basheer S, Selvarajan S. Efficient data transmission on wireless communication through a privacy-enhanced blockchain process. PeerJ Computer Sci. 2023; 9: e1308.
11. Rabie OB, Balachandran PK, Khojah M, Selvarajan S. A proficient ZESO-DRKFC model for smart grid SCADA security. Electronics. 2022; 11 (24): 4144.
12. Aljabhan B, Obaidat MA. Privacy-preserving blockchain framework for supply chain management: Perceptive Craving Game Search Optimization (PCGSO). Sustainability. 2023; 15 (8): 6905.
13. Almasian M, Shafieinejad A. Secure cloud file sharing scheme using blockchain and attribute-based encryption. Computer Standards Interfaces. 2024; 87: 103745.
14. Ren Y, Huang D, Wang W, Yu X. BSMD: A blockchain-based secure storage mechanism for big spatio-temporal data. Future Generation Computer Syst. 2023; 138: 328–338.
15. Chennam K, Muddana L. An efficient two stage encryption for securing personal health records in cloud computing. Int J Services Oper Inform. 2018; 9 (4): 277–296.
16. Xie H, Zheng J, He T, Wei S, Hu C. TEBDS: A trusted execution environment-and-blockchain-supported IoT data sharing system. Future Generation Computer Syst. 2023; 140: 321–330.
17. Ghazal TM, Hasan MK, Abdullah SN, Bakar KA, Taleb N, Al-Dmour NA, Yafi E, Chauhan R, Alzoubi HM, Alshurideh M. An integrated cloud and blockchain enabled platforms for biomedical research. In: Alshurideh M, Al Kurdi, BH, Masa'deh R, Alzoubi HM, Salloum S, editors. The Effect of Information Technology on Business and Marketing Intelligence Systems. Cham, Switzerland: Springer; 2023. pp. 2037–2053.
18. Li Z, Li Y, Lu L, Ding Y. Blockchain-based auditing with data self-repair: from centralized system to distributed storage. J Syst Architect. 2023; 137: 102854.
19. Xu Y, Xiao S, Wang H, Zhang C, Ni Z, Zhao W, Wang G. Redactable blockchain-based secure and accountable data management. IEEE Trans Netw Serv Manage. 2023; 21 (2): 1764–1776.
20. Singh SK, Yang LT, Park JH. FusionFedBlock: fusion of blockchain and federated learning to preserve privacy in industry 5.0. Inform Fusion. 2023; 90: 233–240.
21. Aljumah A, Ahanger TA, Ullah I. Heterogeneous blockchain-based secure framework for UAV data. Mathematics. 2023; 11 (6): 1348.
22. Laghari AA, Khan AA, Alkanhel R, Elmannai H, Bourouis S. Lightweight-biov: blockchain distributed ledger technology (BDLT) for internet of vehicles (IoVs). Electronics. 2023; 12 (3): 677.
23. Mahajan HB. Emergence of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems: solutions, challenges, and future roadmap. Wireless Pers Commun. 2022; 126 (3): 2425–2446.
24. Zuo Y, Kang Z, Xu J, Chen Z. BCAS: A blockchain-based ciphertext-policy attribute-based encryption scheme for cloud data security sharing. Int J Distrib Sensor Netw. 2021; 17 (3): 1550147721999616.

25. Murala DK, Panda SK, Sahoo SK. Securing electronic health record system in cloud environment using blockchain technology. In: Panda SK, Mishra V, Dash SP, Pani AK, editors. Recent Advances in Blockchain Technology: Real-World Applications. Cham, Switzerland: Springer; 2023. pp. 89–116.
26. Kollu PK. Blockchain techniques for secure storage of data in cloud environment. Turk J Computer Math Educ. 2021; 12 (11): 1515–1522.
27. Thirumalaisamy M, Basheer S, Selvarajan S, Althubiti SA, Alenezi F, Srivastava G, Lin JC. Interaction of secure cloud network and crowd computing for smart city data obfuscation. Sensors. 2022; 22 (19): 7169.
28. Chennam KK, Mudanna L. Privacy and access control for security of credit card records in the cloud using partial shuffling. In: 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Chennai, India, December 15–17, 2016. pp. 1–4.
29. Khanna A, Sah A, Bolshev V, Burgio A, Panchenko V, Jasiński M. Blockchain–cloud integration: a survey. Sensors. 2022; 22 (14): 5238.
30. Siddiqui ST, Shuaib M, Gupta AK, Alam S. Implementing blockchain technology: way to avoid evasive threats to information security on cloud. In: 2020 International Conference on Computing and Information Technology (ICCIT–1441), Tabuk, Saudi Arabia, September 9–10, 2020. pp. 1–5.
31. Xu H, Cao J, Zhang J, Gong L, Gu Z. A survey: cloud data security based on blockchain technology. In: 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC), Hangzhou, China, June 23–25, 2019. pp. 618–624.
32. Cheng R, Zhang F, Kos J, He W, Hynes N, Johnson N, Juels A, Miller A, Song D. Ekiden: a platform for confidentiality-preserving, trustworthy, and performant smart contracts. In: 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, June 17–19, 2019. pp. 185–200.
33. Stodt J, Reich C. Data confidentiality in P2P communication and smart contracts of blockchain in Industry 4.0. arXiv preprint. arXiv:2007.14195. July 28, 2020. Available at https://arxiv.org/abs/2007.14195
34. Mann S, Potdar V, Gajavilli RS, Chandan A. Blockchain technology for supply chain traceability, transparency and data provenance. In: Proceedings of the 2018 International Conference on Blockchain Technology and Application, Xi'an, China, December 10–12, 2018. pp. 22–26.
35. Song ZH, Yang LI, Gaoyang LI, Han YU, Baozhong HA, Jinwei SO, Jingang FA. An improved data provenance framework integrating blockchain and PROV model. In: 2020 International Conference on Computer Science and Management Technology (ICCSMT), Shanghai, China, November 20–22, 2020. pp. 323–327.
36. Jamil F, Ahmad S, Iqbal N, Kim DH. Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. Sensors. 2020; 20 (8): 2195.
37. Ronaghi MH. Contextualizing the impact of blockchain technology on the performance of new firms: the role of corporate governance as an intermediate outcome. J High Technol Manage Res. 2022; 33 (2): 100438.
38. Saygili M, Mert IE, Tokdemir OB. A decentralized structure to reduce and resolve construction disputes in a hybrid blockchain network. Automation Construct. 2022; 134: 104056.
39. Wang X, Yao F, Wen F. Applications of blockchain technology in modern power systems: a brief survey. Energies. 2022; 15 (13): 4516.
40. Kaushik K, Dahiya S, Sharma R. Role of blockchain technology in digital forensics. In: Vyas S, Shukla VK, Gupta S, Prasad A, editors. Blockchain Technology. Boca Raton, FL, USA: CRC Press; 2022. pp. 235–246.
41. Li C, Zhang J, Yang X. Scalable blockchain storage mechanism based on two-layer structure and improved distributed consensus. J Supercomputing. 2022; 78: 4850–4881.

