International Multidisciplinary Research Journal Reviews (IMRJR)

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 3, March 2025
DOI 10.17148/IMRJR.2025.020308

Blockchain for Secure Cloud Storage & IoT Infrastructure: The Future of Decentralization

Gouni Sushma

Department of Computer Science and Engineering, Vaagdevi Engineering College

Abstract: Blockchain technology creates a new way to store data that solves typical cloud storage problems by running data across multiple devices. Users can get better security for their data, while trust in single breakdowns decreases when they store data through blockchain-distributed ledgers. Data management becomes more trustworthy on blockchain-based cloud storage because its decentralized architecture provides greater privacy protection and data control. Researchers now study ways blockchain works with cloud storage across different applications such as healthcare, IoT devices, and digital forensics. The complete adoption of blockchain-based storage requires us to overcome scalability, communication, and legal difficulties.

1. INTRODUCTION

Companies and individuals choose cloud storage because data production increases while they need secure and dependable storage options[1]. Past cloud storage systems based on a centralized model create important worries about personal data safety, protection, and ownership. People worry their data might get stolen or exposed while others can illegally access it, and they do not see their files clearly. Blockchain technology presents an effective answer to data management challenges because it provides users with secure distributed storage services[2,3,4]. Users benefit from blockchain when it stores data safely because multiple computers keep records, whereas centralization failures decrease while users maintain strong data authority. The decentralized cloud storage system overcomes traditional cloud storage issues and creates better ways to control data safely.

2. THEORETICAL FRAMEWORK OF BLOCKCHAIN TECHNOLOGY

A blockchain system tracks network transactions using multiple connected computers that do not depend on central control. Users trust blockchain because its system cannot be changed, and everyone can see each transaction. It also guards against unauthorized access. Because of its distributed design, Blockchain creates a dependable way for users to exchange information securely among peers. Blockchain technology creates a safe platform that lets different users share information without needing a single controlling organization[5,6,7]. A distributed system like blockchain protects data better and prevents technical failures while letting users govern their information[8,9,10]. The decentralized design of blockchain brings multiple pros that protect user data better while reducing dependence on single systems and enhancing control over personal records[11]. By noting each transaction and data owner on the blockchain ecosystem, users can easily detect any misuse or theft of information[12,13]. Data is better protected from single failure points since the regular cloud storage approach does not rely on a single location. In blockchain, every new block stores a hash or unique identifier that links back to its preceding block, creating an unbroken chain [14].

Characteristic	Description
Decentralization	Blockchain systems do not rely on a central authority to manage transactions and data. Instead, the network of participants collectively maintains and verifies the ledger.
Immutability	Once data is recorded on the blockchain, it becomes extremely difficult to modify or delete, ensuring the integrity of the information.
Transparency	All transactions on the blockchain are visible to participants, promoting trust and accountability.
Distributed Ledger	The blockchain acts as a distributed database, where copies of the ledger are maintained across multiple nodes in the network.
Cryptography	Blockchain utilizes cryptographic techniques to secure data and protect against unauthorized access or tampering.

3. CURRENT RESEARCH ON BLOCKCHAIN FOR CLOUD STORAGE

Research now investigates how blockchain technology can work with cloud storage solutions to improve the standard cloud storage approaches[15,16]. The research presents a storage system that applies blockchain together with cloud storage methods for managing personal health data in a protected decentralized format[17].

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 3, March 2025
DOI 10.17148/IMRJR.2025.020308

A blockchain-based IoT structure is analyzed in research to demonstrate how it provides safe, decentralized data management capabilities for IoT networks.

Use Case	Description
Data Security	Blockchain technology improves data security in cloud storage systems by distributing data across multiple nodes and securing it through cryptographic methods.
User Control	Decentralized cloud storage systems enable users to have complete control over their data through direct permission management and evidence tracking of their information.

Moreover, studies have investigated blockchain applications within digital forensics to validate digital evidence as well as maintain its provenance since this becomes essential when examining cloud storage systems[18]. Multiple studies from the literature confirm that blockchain integrated with cloud storage delivers a safe distributed system that benefits numerous domains, including healthcare, IoT, and digital forensics. A combination of blockchain technology and cloud storage features a promising solution to decentralize secure data handling systems by solving traditional storage model problems[19]. The distributed structure and secure nature of blockchain enable researchers to establish new applications, which include health solutions, IoT systems, and digital evidence management. In the realm of cloud storage, digital evidence needs reliable systems to maintain evidence authenticity and track its origins. Continuous advancement in research will shape the prospect of decentralized cloud storage with blockchain technology to offer greater data safety along with user authority and improved trust in cloud data management.

4. GAPS IN EXISTING BLOCKCHAIN CLOUD STORAGE SOLUTIONS

The current research about blockchain-based cloud storage solutions generates promising outcomes, but researchers must overcome multiple gaps and technical challenges. The expanding number of blockchain transactions combined with data storage requirements creates scalability problems that produce performance bottlenecks[20]. The merger between blockchain and cloud storage systems requires developers to handle the technical difficulty associated with making their systems talk to each other smoothly.

The regulatory and legal guidelines concerning blockchain and cloud storage implementation must be carefully examined. Public sector entities require solutions to handle data privacy concerns and legal boundaries that enforce blockchain usage in contracts and transactions, as well as cross-border data movement regulations. The implementation of blockchain-based cloud storage faces challenges since some users do not understand this technology and also doubt its security and reliability aspects[21]. Widespread adoption of blockchain-based cloud storage solutions requires successful efforts to overcome user skepticism and prove their reliability and security features to users. Many individuals need in-depth educational sessions about how the technology works, along with demonstrations of its abilities and risk-reduction actions for uncertainties[22]. The hypergrowth of decentralized cloud storage systems requires legal frameworks that guarantee enforceability for blockchain transactions, together with clear rules and regulations, to build user trust. The solution to these issues will enable blockchain-enhanced cloud storage to bring secure user-oriented data management solutions with transparency to the market.

The decentralized method holds advantages, including better data protection, decreased chances of a single failure point, and increased user control over the information stored[23]. The data management process becomes more transparent along with being trustworthy through blockchain because the blockchain system uses distributed ledgers to record ownership information and transaction histories[24]. The distributed architecture helps minimize cloud storage risk elements that include single-point outages together with data privacy threats and control problems over sensitive data. Research shows that blockchain combined with cloud storage presents a hopeful future for secure decentralized data management since it solves traditional cloud storage issues. The decentralized nature of blockchain enables researchers to establish different applications that depend on its transparent and tamperproof characteristics in healthcare services IoT systems, as well as digital forensic analysis[25]. Digital evidence integrity, together with traceability, stands as the most important aspect of cloud storage systems. Research in decentralized cloud storage with blockchain keeps developing toward delivering enhanced data protection alongside user autonomy and improved trust for cloud platform data management.

5. THE FUTURE OF DECENTRALIZED CLOUD STORAGE WITH BLOCKCHAIN

The integration of blockchain technology with cloud storage offers a compelling vision for the future of decentralized and secure data management[26]. By leveraging the decentralized, transparent, and tamper-resistant properties of blockchain, this approach can address the limitations of traditional cloud storage models and provide several key benefits:

1. Data security gets improved when blockchain technology powers cloud storage systems because data spreads across multiple nodes, thus securing information through cryptographic method [27].
2. De-centralized cloud storage systems enable users to achieve complete control over their data through direct permission management and evidence tracking of their information[28].

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 3, March 2025
DOI 10.17148/IMRJR.2025.020308

3. Users benefit from blockchain-based cloud storage because it enables clear tracking of data transactions combined with auditable access log records[29]. Blockchain-based cloud storage provides users with an audit functionality that enhances their trust while demanding accountability from the system[30].
4. The main benefit of this approach includes minimizing the possibility of system breakdowns due to centralized service providers and servers becoming single points of failure[31].
5. Mass storage facilities become safer through blockchain-based decentralized cloud storage systems, which spread information and storage across multiple network nodes[32]. Blockchain research development continues to advance at a fast pace, with numerous promising prospects to offer secure, accessible data management services to users.

The use of blockchain to secure cloud storage is being viewed as a solution to address technology concerns, such as decentralization, identity, data ownership, and information-driven choices [33]. Blockchain introduces a safe method for providing Internet of Things services and decentralized data control solutions. As blockchain technology develops, smartphones and tablets are becoming more sophisticated and require forensic investigations that are able to create, store, transport, utilize, and modify evidence in order to maintain its original character [34].

6. CONCLUSION

The future of managed data stands promising because blockchain technology integrates effectively with cloud storage capabilities. This method shows potential to solve cloud storage issues through blockchain system benefits, which include decentralization and transparent and tamper-proof functionality. Blockchain-based cloud storage obtains enhanced data security by spreading data among multiple nodes while using cryptography to secure control of user data and improve digital information traceability. Decentralized cloud storage with blockchain technology will continue to develop as an effective solution for modern data management and securing information in the cloud.

REFERENCES

[1]. P. Pawar, D. Kumar, M. K. Meesala, P. K. Pareek, S. R. Addula, and K. S. Shwetha, “Securing Digital Governance: A Deep Learning and Blockchain Framework for Malware Detection in IoT Networks,” Nov. 22, 2024. doi: 10.1109/iciics63763.2024.10860155.

[2]. Konda, B., Yenugula, M., Kasula, V. K., & Yadulla, A. R. (2024). A Public Key Searchable Encryption Scheme Based on Blockchain Using Random Forest Method. *International Journal Of Research In Electronics And Computer Engineering*, *12*(1), 77-83.

[3]. D. Manikandan, C. Valliyammai, and R. N. Karthika, “Blockchain-based Secure Big Data Storage on Cloud,” Nov. 26, 2020. doi: 10.35940/ijrte.d4744.119420.

[4]. Addula, S. R., Tyagi, A. K., Naithani, K., & Kumari, S. (2024). Blockchain-empowered Internet of things (IoTs) platforms for automation in various sectors. *Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing*, 443-477. https://doi.org/10.1002/9781394303601.ch20

[5]. S. Srivastava, M. Pant, S. K. Jauhar, and A. K. Nagar, “Analyzing the Prospects of Blockchain in Healthcare Industry,” Computational and Mathematical Methods in Medicine, vol. 2022. Hindawi Publishing Corporation, p. 1, Dec. 02, 2022. doi: 10.1155/2022/3727389.

[6]. S. E. Vadakkethil, K. Polimetla, Z. Alsalami, P. K. Pareek, and D. Kumar, “Mayfly Optimization Algorithm with Bidirectional Long-Short Term Memory for Intrusion Detection System in Internet of Things,” Apr. 26, 2024. doi: 10.1109/icdcece60827.2024.10549401.

[7]. Yadulla, A. R., Yenugula, M., Kasula, V. K., Konda, B., Addula, S. R., & Rakki, S. B. (2023). A time-aware LSTM model for detecting criminal activities in blockchain transactions. International Journal of Communication and Information Technology 2023; 4(2): 33-39

[8]. H. Gonaygunta, D. Kumar, S. Maddini, and S. F. Rahman, “How can we make IoT Applications better with Federated Learning- A Review,” IJARCCE, vol. 12, no. 2. Feb. 20, 2023. doi: 10.17148/ijarcce.2023.12213.

[9]. B. Ram and P. Verma, “Application of blockchain technology in data security,” Aug. 03, 2024. doi: 10.18231/j.ijlsit.2024.008.

[10]. Almotairi, S., Addula, S. R., Alharbi, O., Alzaid, Z., Hausawi, Y. M., & Almutairi, J. (2024). Personal data protection model in IOMT-blockchain on secured bit-count transmutation data encryption approach. *Fusion: Practice and Applications*, *16*(1), 152-170. https://doi.org/10.54216/fpa.160111

[11]. P. Pawar, D. Kumar, R. K. Bhujang, P. K. Pareek, H. M. Manoj, and K. Deepika, “Investigation on Digital Forensic Using Graph-Based Neural Network With Blockchain Technology,” Jul. 26, 2024. doi: 10.1109/icdsns62112.2024.10691122.

[12]. Kasula, V. K. (2022). Empowering Finance: Cloud Computing Innovations in the Banking Sector. International Journal of Advanced Research in Science Communication and Technology, 2(1): 877-881

[13]. Z. Liu, “Application of Blockchain and Distributed Storage Technology,” Sep. 30, 2022. doi: 10.54097/hset.v9i.1713.

[14]. Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-Based Medical Records Secure Storage and Medical Service Framework," Nov. 22, 2018, Springer Science+Business Media. Doi: 10.1007/s10916-018-1121-4.

[15]. Y. Wenqi, J. Shen, Z. Cao, and X. Dong, "Blockchain-Based Digital Evidence Chain of Custody," Mar. 12, 2020. doi: 10.1145/3390566.3391690.

[16]. Y. Kang and Q. Li, "Design and Implementation of Data Sharing Traceability System Based on Blockchain Smart Contract," Nov. 15, 2021, Hindawi Publishing Corporation. doi: 10.1155/2021/1455814.

[17]. K. Patibandla, R. Daruvuri, and P. Mannem, "Streamlining workload management in AI-driven cloud architectures: A comparative algorithmic approach," *International Research Journal of Engineering and Technology*, vol. 11, no. 11, pp. 113-121, 2024.

[18]. C. Pandey, "Scalability Challenges and Opportunities in Blockchain-based Systems: A Systematic Review," Türk bilgisayar ve matematik eğitimi dergisi, vol. 11, no. 3. Karadeniz Technical University, p. 2022, Dec. 15, 2020. doi: 10.17762/turcomat.v11i3.13599.

[19]. Konda, B., Kasula, V. K., Yenugula, M., Yadulla, A. R., & Addula, S. R. (2022). Homomorphic encryption and federated attribute-based multi-factor access control for secure cloud services in integrated space-ground information networks.

[20]. D. Kumar, P. Pawar, A. Bhuvanesh, S. Indhumathi, and M. Murugan, "ChOs_LSTM: Chebyshev Osprey Optimization-Based Model for Detecting Attacks," May 03, 2024. doi: 10.1109/aiiot58432.2024.10574586.R. Daruvuri, "Automating repetitive tasks in cloud-based AI systems: A deep learning perspective," *International Journal of Computer Science and Mechatronics*, vol. 11, no. 1, pp. 1-7, 2025.

[21]. M. M. Merlec and H. P. In, "Blockchain-Based Decentralized Storage Systems for Sustainable Data Self-Sovereignty: A Comparative Study," Sep. 04, 2024, Multidisciplinary Digital Publishing Institute. doi: 10.3390/su16177671.

[22]. R. Zhang, R. Xue, and L. Liu, "Security and Privacy for Healthcare Blockchains," Jun. 02, 2021, Institute of Electrical and Electronics Engineers. doi: 10.1109/tsc.2021.3085913.

[23]. P. Sharma, R. Jindal, and M. D. Borah, "Blockchain Technology for Cloud Storage," ACM Computing Surveys, vol. 53, no. 4. Association for Computing Machinery, p. 1, Aug. 03, 2020. doi: 10.1145/3403954.

[24]. P. Patil, P. Tulsiani, and S. B. Mane, "Mitigating Data Sharing in Public Cloud using Blockchain," Apr. 21, 2024, Cornell University. doi: 10.48550/arXiv.2404.

[25]. S. Kanatt, P. Talwar, and A. Jadhav, "Review of Secure File Storage on Cloud using Hybrid Cryptography," Feb. 08, 2020, International Research Publication House. doi: 10.17577/ijertv9is020014.

[26]. C. Li, J. Hu, K. Zhou, W. Yuan-zhang, and H. Deng, "Using Blockchain for Data Auditing in Cloud Storage," in Lecture notes in computer science, Springer Science+Business Media, 2018, p. 335. doi: 10.1007/978-3-030-00012-7_31.

[27]. M. Marwan, A. Kartit, and H. Ouahmane, "A Framework to Secure Medical Image Storage in Cloud Computing Environment," Dec. 26, 2017, IGI Global. doi: 10.4018/jeco.2018010101.

[28]. Yadulla, A. R. (2022). Building smarter firewalls: Using AI to strengthen network security protocols. Int J Comput Artif Intell, 3(2):109-112

[29]. M. G. Jaatun, I. A. Tøndel, N. B. Moe, D. S. Cruzes, K. Bernsmed, and B. Haugset, "Accountability Requirements in the Cloud Provider Chain," Apr. 20, 2018, Multidisciplinary Digital Publishing Institute. doi: 10.3390/sym10040124.

[30]. H. S. Musa, M. Krichen, A. A. Altun, and M. Ammi, "Survey on Blockchain-Based Data Storage Security for Android Mobile Applications," Sensors, vol. 23, no. 21. Multidisciplinary Digital Publishing Institute, p. 8749, Oct. 26, 2023. doi: 10.3390/s23218749.

[31]. Addula, S. R., Meduri, K., Nadella, G. S., & Gonaygunta, H. (2024). AI and blockchain in finance: Opportunities and challenges for the banking sector. *IJARCCE*, *13*(2). https://doi.org/10.17148/ijarcce.2024.13231

[32]. R. Daruvuri, "Dynamic load balancing in AI-enabled cloud infrastructures using reinforcement learning and algorithmic optimization," World Journal of Advanced Research and Reviews, vol. 20, no. 1, pp. 1327–1335, Oct. 2023, doi: 10.30574/wjarr.2023.20.1.2045.

[33]. Yenugula, M. (2022). Google Cloud Monitoring: A Comprehensive Guide. Journal of Recent Trends in Computer Science and Engineering (JRTCSE), vol. 10, no. 2, pp. 40-50

[34]. Konda, B. (2022). The Impact of Data Preprocessing on Data Mining Outcomes. World Journal of Advanced Research and Reviews, 15(3): 540-544, https://doi.org/10.30574/wjarr.2022.15.3.0931