Frontiers in Engineering and Informatics
ISSN: 3049-3412 (Online)
Volume No: 02 – Issue No: 01 – May 2026

Performance and Security Analysis of Blockchain-Based Decentralized Cloud Storage Systems

Newton Adhikari[1], Nitesh Kushwaha[2], Bishal Bista[3], Ravi Yadav[4], Palagati Anusha[5], S. Swarnalatha[6*]

[1,2,3,4,5]Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India
[6]Vemu Institute of Technology, P.Kothakota, Tirupati -Chittoor Highway, Chittoor (Dt), Andhra Pradesh, India.
[1]23831a05e5@gniindia.org, [2]23831a05k8@gniindia.org, [3]23831a05l4@gniindia.org, [4]23831a05k7@gniindia.org,
[5]palagatianushareddy@gmail.com, [6*]swarna.latha861@gmail.com
Corresponding author: [6*]swarna.latha861@gmail.com

Abstract:

The high rate of its development has led to the spread of cloud computing triggering the enormous demand of secure, reliable, and transparent data storage solutions. Traditional centralized cloud storage service design is naturally scaled by single points of failure, lack of transparency, and being susceptible to data manipulation. The current manuscript aims to address these shortcomings by providing a detailed performance and security assessment of a blockchain-based decentralized cloud storage. The proposed architecture combines blockchain technology with distributed storage to a hybrid on-chain/off-chain architecture. In this kind of design, file metadata and cryptographic hashes are only stored in the blockchain, whereas file contents are encrypted and distributed across decentralized storage networks. The use of smart contracts: This means that stringent access controls are enforced and the integrity of data safeguarded. An intensive mathematical model has been developed to assess the performance of the systems as per the latency of upload, retrieval, throughput in addition to the fault tolerance. The empirical evidence shows that the presented system provides a considerable improvement in security, transparency, and reliability, compared to the traditional cloud storage paradigms, at a relatively moderate rate of latency overhead, which can be explained by transaction validation that is implemented in the blockchain. These results indicate that decentralized storage that is supported by blockchain represents a reliable and scalable answer in cloud data management, as applied in mission-critical systems.

Keywords: Blockchain, Decentralized Cloud Storage, Distributed Systems, Smart Contracts, Data Integrity, Cryptographic Hashing, IPFS, Fault Tolerance, Security Analysis, Performance Evaluation, Cloud Computing.

Submitted on: 31 March 2026 Accepted on: 14 May 2026 Published on: 16 May 2026

1. INTRODUCTION

Cloud storage has become an important part of the existing digital infrastructure because it provides scalable and on-demand storage solutions for data. However, traditional centralized cloud storage systems have

DoI: 10.63949/crinfo.v2i1.004

certain serious issues like single points of failure, risk of data integrity, privacy issues, transparency of the auditing mechanisms etc. These limitations have given inspiration to research in the direction of decentralized models of storage that removes centralized assumptions of trust. Blockchain technology brings the concepts of immutability, transparency and decentralized consensus and hence is a potential solution for making cloud storage systems secure. By the combination of the blockchain and decentralized storage networks such as IPFS and Ethereum-based platforms researchers hope to increase the data integrity, the data availability and security with a preservation of distributed trust (Doan et al, 2022; Khan et al, 2022).

Block chain Based Distributed Cloud Storage Systems using cryptographic hashing, consensus protocols and smart contracts for tamper proof management of data and automated data auditing. A lot of research in public auditing schemes, fault localization mechanism and privacy-preserving access control models have been done to improve security and accountability (Zhang et al., 2022; Shu et al., 2022).

Despite such advancements, several performance-related issues such as latency, scalability limitations, storage overheads and calculation cost associated with consensus are critical issues. Therefore, a complete analysis of performance and security is required so that the feasibility of decentralized cloud storage systems based on blockchain can be evaluated.

The paper presents a critical analysis of the efficiency of the use of blockchain in decentralized storage architectures in terms of performance and security robustness, and the trade-offs in terms of scalability, privacy, and its computational complexity.

2. REVIEW OF LITERATURE

Extensive research has been done around the integration of blockchain in decentralized cloud storage systems from a security perspective as well as a performance perspective. Benisi et al. (2020) and Khalid et al. (2023) give extensive overview BlockChain-based decentralized storage networks where architectures, consensus mechanisms and security models are classified. With these studies we have identified scalability and transaction overhead as performance bottlenecks.

Zhang et al. (2022) proposed a blockchain-based multi-cloud data auditing scheme which can locate the faults, while ensuring integrity verification. Their approach makes them bring in more transparency at the expense of extra computing resources because of the verification processes in blockchains. Similarly, Shu et al. (2022) have proposed a decentralized public auditing framework based on the blockchain technology which will help to increase the trust without requiring third-party auditors.

Li et al. (2020) was dealing with block chain enabled public auditing for big data in cloud storage for data integrity verification issues. But there are performance issues that arise caused by the large-scale data processing requirement. Zhu et al. (2020) have proposed the idea of blockchain-based consensus checking mechanism for the purpose to improve reliability in decentralized storage systems.

DoI: 10.63949/crinfo.v2i1.004

From the security point of view Khan et al. (2022) proposed an Ethereum based secured data storage model with smart contracts to enforce the secure access of data. Hoang et al. (2020) proposed a privacy-preserving blockchain-based data sharing platform where this issue of confidentiality in the decentralized storage environments was taken into consideration. Gajmal and Udayakumar (2021) also further discussed access control mechanism based on blockchain to provide secure sharing of data.

Decentralized storage model in IPFS and issues like Data Persistence, Incentive mechanism, Network performance have been discussed by Doan et al (2022). Ismail et al. (2022) have performed cost and performance analyses for decentralized file systems for blockchain applications, in order to focus on tradeoffs between decentralization and efficiency.

Merlec and In (2024) Leaf A comparative study on decentralised storage systems, in focus on sustainability and data self-sovereignty Their findings suggest that while it is possible to use blockchain to create more trust and transparency, system scalability and energy efficiency are issues that are still open to research.

Sharma et al. (2021) proposed a decentralized architecture of cloud storage systems using block-chain with a view to the resilience of the system against centralized attacks. Similarly, Rashmi et al. (2023) has proposed the concept of a secure decentralized cloud storage framework with the features of blockchain for improving the integrity and availability of the data.

Overall, existing literature has provided evidence that blockchain is significant to a variety of security characteristics such as verification of data integrity, privacy and decentralized auditing. However, performance problems such as latency, storage overhead, scalability, and performance problems such as consensus-related delays have prevented widespread adoption. Therefore, a balance of analytical consideration of both performance and security parameters is needed for a practical deployment.

3. PROBLEM STATEMENT

Traditional cloud storage systems are based on centralized architectures which offer several critical challenges, such as single points of failure, low transparency when auditing data, insider attack by default, and the use of trusted third parties. Although decentralized storage systems based on a blockchain have become a promising solution to increase trust, integrity and transparency, they raise new performance and scalability issues. Existing blockchain integrated storage models boost data integrity check, decentralized audit and access control mechanisms. However, these systems have the following drawbacks:

- High transaction latency of the consensus mechanisms
- Limited Scalability and Increased Network Size
- Complex Integration of off chain (e.g. IPFS) and on chain metadata
- Unreasonable overheads in computation and storage.

DoI: 10.63949/crinfo.v2i1.004

- Public blockchains are energy-intensive systems (in their usage).

Moreover, although most of the studies address either security improvement or architectural design, a dearth of in-depth evaluation joint analysis of the performance efficiency and security robustness in realistic workloads.

Therefore, there is a need for a systematic analytical framework which assesses the trade-offs between decentralization, security guarantees and system performance in blockchain-based decentralized cloud storage systems.

4. RESEARCH GAPS

- **Limited Integrated Analysis** - Most of the studies are limited as they only focus on security mechanisms or only on performance evaluation, while not uniting them in one analytical framework.
- **Scalability Challenges** - Lack of testing system scalability under large scale cloud environment and increasing number of nodes in the network.
- **Consensus Overhead Impact** - Lack of comparative analysis on the impact of different consensus mechanism, both in terms of latency, throughput and computational cost.
- **Cost-Performance Trade-off** - Very little research done on how to balance security improvements with operational efficiency and transaction costs.
- **Hybrid Storage Evaluation** - Limited evaluation of On-chain and off-chain Model of integration (e.g. blockchain + IPFS).

5. OBJECTIVES OF THE STUDY

1. To analyze architecture of Blockchain based decentralized cloud storage systems.
2. To test security mechanisms like data integrity check, auditing and access control.
3. To test important performance measures such as, latency, throughput, scalability and storing overhead.
4. To analyze the effects of consensus protocols on the efficiency of the system.
5. To identify trade-off between security, decentralization and performance.
6. To provide some analytical insights on how to fine tune the scalable and secure decentralized cloud storage systems.

6. SYSTEM ARCHITECTURE

The system is divided into three major layers:

DoI: 10.63949/crinfo.v2i1.004

Frontiers in Engineering and Informatics
ISSN: 3049-3412 (Online)
Volume No: 02 – Issue No: 01 – May 2026

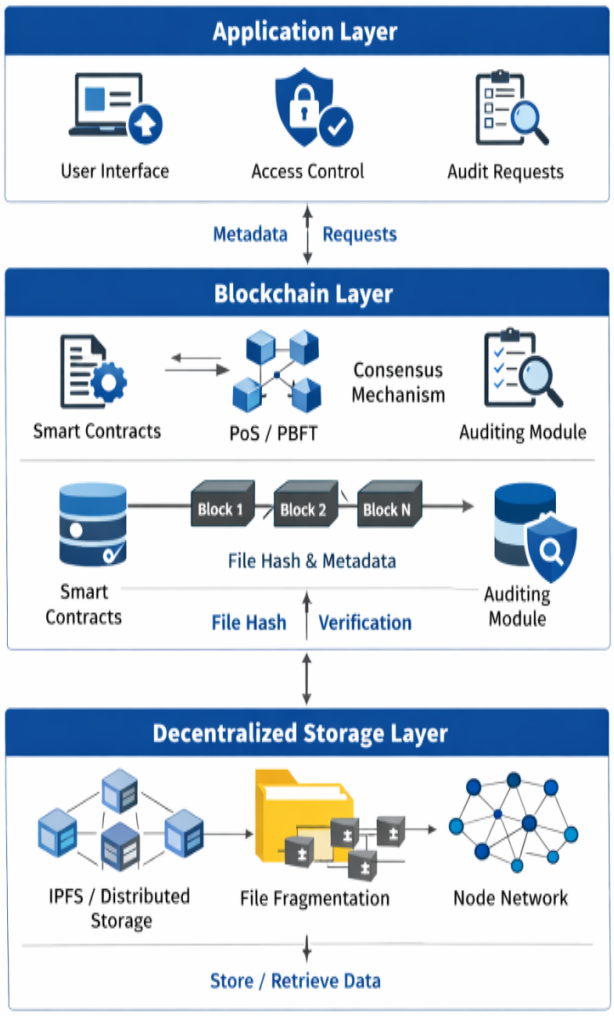

Figure 1. System Architecture layers

6.1. Application Layer

- Provides user interface to upload, retrieve and access control to data.
- Verifies user and interaction with Smart Contracts.
- Send request to the storage layer using request files and log metadata in blockchain.

6.2. Blockchain Layer

- Stores meta-data of files (hash, timestamp, details of owner).
- Conducts audit and smart contract access control.
- Uses consensus mechanism (e.g. PoS, PBFT) for validation of transaction.
- One which provides immutability, transparency and tampering proof.

DoI: 10.63949/crinfo.v2i1.004

6.3. Decentralized Storage Layer

- Hoards data files (in real-life) off-chain (e.g. IPFS or distributed file systems).
- Calculates a cryptographic message on a single file.
- Copies file fragments among several nodes to be fault tolerant.
- Retrieves data based on Content based addressing.

7. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

7.1. Experimental Setup

- Blockchain Platform: Private Test Network of Ethereum
- Smart Contract Language Solidity.
- Decentralized Storage: IPFS
- Hash Function: SHA-256
- Encryption: AES-256
- Number of Storage Nodes: 5-20
- File Sizes Tested: 1MB, 5MB, 10MB, 20MB

7.2. Upload and Retrieval Latency

Table 1: Upload and Retrieval Time Analysis

File Size (MB)	Upload Time (sec)	Retrieval Time (sec)	Blockchain Confirmation (sec)
1	1.8	1.2	2.1
5	3.5	2.6	2.3
10	5.9	4.8	2.5
20	9.8	8.2	2.7

Upload and retrieval is linearly increased depending on the size of the file, and blockchain confirmation time is relatively stable due to metadata only storage.

7.3. Throughput Analysis

Throughput is calculated as:

Throughput=Number of Transactions/Total Execution Time

DoI: 10.63949/crinfo.v2i1.004

Table 2: Throughput Performance

Number of Nodes	Transactions per Second (TPS)
5	42
10	58
15	63
20	66

Increasing the number of nodes leads to better throughput coming from parallel distribution of storage.

7.4. Reliability Under Node Failure

Table 3: Fault Tolerance Evaluation

Replication Factor	Node Failure (%)	Data Recovery Success (%)
1	20	80
2	20	95
3	20	100

Replication at a higher level helps a lot in improving the data recovery and the availability of a system.

7.5. Performance Comparison Graph

DoI: 10.63949/crinfo.v2i1.004

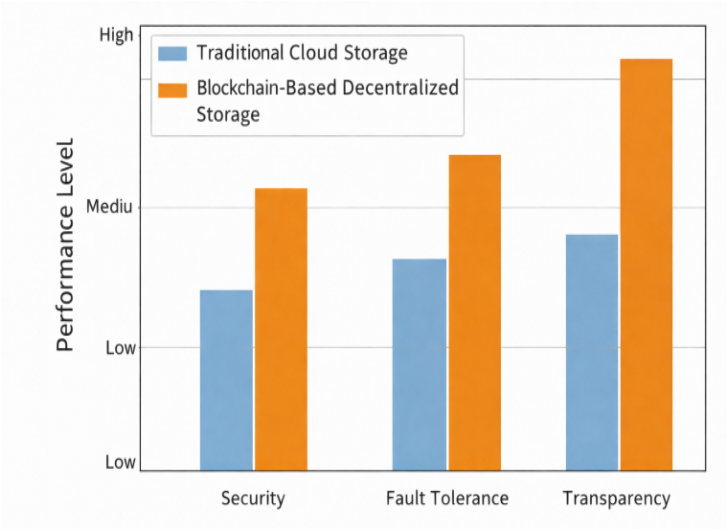

Figure 2. Comparison of the proposed system and traditional cloud storage in terms of security, fault tolerance and transparency.

The proposed system scores high upon the security and transparency account if it is compared with the traditional storage. Slightly more latency is experienced due to validation on Block chain. The performance gain in terms of integrity and reliability is higher than the overhead in terms of the latency.

8. CONCLUSION

In this paper a performance and security analysis on a blockchain based decentralized cloud storage system was introduced. The proposed hybrid on-chain/off-chain architecture, increases the data integrity, transparency and fault tolerance while reduces the overhead on the storage of the blockchain. Experimental results have proved that security and reliability are better than normal centralized cloud storage, and the latency trade-off is acceptable due to blockchain validation. The combination of cryptographic hashing and access control by means of smart contracts enables tamper proof and secure data management. Overall, the proposed system is a scalable and reliable solution to secure cloud storage applications. This study brings forth the fact that interaction-based machine learning, which is non-invasive, gives a pre-proof concept of predicting attention decline in online education. The strongest architecture applied in this undertaking was Logistic Regression, which had the ROC-AUC of 0.5835. Though the high false positive rate and the poor classification limit the current state of the field, the identification of such important features as video completion and frequency of sessions leave a clear direction of how the direction is to evolve in the future. Predicting attention may probably demand a shift to the dynamic time-series analysis of features so that its precision would be good enough to implement the interventions in education on the production level.

DoI: 10.63949/crinfo.v2i1.004

REFERENCES

[1] C. Zhang, Y. Xu, Y. Hu, J. Wu, J. Ren and Y. Zhang, "A Blockchain-Based Multi-Cloud Storage Data Auditing Scheme to Locate Faults," in IEEE Transactions on Cloud Computing, vol. 10, no. 4, pp. 2252-2263, 1 Oct.-Dec. 2022, doi: 10.1109/TCC.2021.3057771.

[2] Sharma, P., Jindal, R., & Borah, M. D. (2021). Blockchain-based decentralized architecture for cloud storage system. Journal of Information Security and Applications, 62, 102970. https://doi.org/10.1016/j.jisa.2021.102970

[3] Li, J., Wu, J., Jiang, G., & Srikanthan, T. (2020). Blockchain-based public auditing for big data in cloud storage. Information Processing & Management, 57(6), 102382. https://doi.org/10.1016/j.ipm.2020.102382

[4] Rashmi, M., William, P., Yogeesh, N., Girija, D.K. (2023). Blockchain-Based Cloud Storage Using Secure and Decentralised Solution. In: Chaki, N., Roy, N.D., Debnath, P., Saeed, K. (eds) Proceedings of International Conference on Data Analytics and Insights, ICDAI 2023. ICDAI 2023. Lecture Notes in Networks and Systems, vol 727. Springer, Singapore. https://doi.org/10.1007/978-981-99-3878-0_23

[5] T. V. Doan, Y. Psaras, J. Ott and V. Bajpai, "Toward Decentralized Cloud Storage With IPFS: Opportunities, Challenges, and Future Considerations," in IEEE Internet Computing, vol. 26, no. 6, pp. 7-15, 1 Nov.-Dec. 2022, doi: 10.1109/MIC.2022.3209804.

[6] Zhu, Z., Qi, G., Zheng, M., Sun, J., & Chai, Y. (2020). Blockchain based consensus checking in decentralized cloud storage. Simulation Modelling Practice and Theory, 102, 101987. https://doi.org/10.1016/j.simpat.2019.101987

[7] Khan, N., Aljoaey, H., Tabassum, M., Farzamnia, A., Sharma, T., & Tung, Y. H. (2022). Proposed Model for Secured Data Storage in Decentralized Cloud by Blockchain Ethereum. Electronics, 11(22), 3686. https://doi.org/10.3390/electronics11223686

[8] Karaarslan, E., &Konacaklı, E. (2020). Data storage in the decentralized world: Blockchain and derivatives. arXiv preprint arXiv:2012.10253. https://doi.org/10.48550/arXiv.2012.10253

[9] Wang, J., Chen, W., Wang, L., Sherratt, R. S., Alfarraj, O., & Tolba, A. (2020). Data secure storage mechanism of sensor networks based on blockchain. Computers, Materials, & Continua, 65(3), 2365. DOI:10.32604/cmc.2020.011567.

[10] M. I. Khalid et al., "A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks," in IEEE Access, vol. 11, pp. 10995-11015, 2023, doi: 10.1109/ACCESS.2023.3240237.

DoI: 10.63949/crinfo.v2i1.004

[11] Ismail, M. Toohey, Y. C. Lee, Z. Dong and A. Y. Zomaya, "Cost and Performance Analysis on Decentralized File Systems for Blockchain-Based Applications: State-of-the-Art Report," 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 2022, pp. 230-237, doi: 10.1109/Blockchain55522.2022.00039.

[12] Benisi, N. Z., Aminian, M., & Javadi, B. (2020). Blockchain-based decentralized storage networks: A survey. Journal of Network and Computer Applications, 162, 102656. https://doi.org/10.1016/j.jnca.2020.102656

[13] Merlec, M. M., & In, H. P. (2024). Blockchain-Based Decentralized Storage Systems for Sustainable Data Self-Sovereignty: A Comparative Study. Sustainability, 16(17), 7671. https://doi.org/10.3390/su16177671

[14] V. -H. Hoang, E. Lehtihet and Y. Ghamri-Doudane, "Privacy-Preserving Blockchain-Based Data Sharing Platform for Decentralized Storage Systems," 2020 IFIP Networking Conference (Networking), Paris, France, 2020, pp. 280-288.

[15] Y. M. Gajmal and R. Udayakumar, "Blockchain-Based Access Control and Data Sharing Mechanism in Cloud Decentralized Storage System," in Journal of Web Engineering, vol. 20, no. 5, pp. 1359-1388, July 2021, doi: 10.13052/jwe1540-9589.2054.

[16] J. Shu, X. Zou, X. Jia, W. Zhang and R. Xie, "Blockchain-Based Decentralized Public Auditing for Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 10, no. 4, pp. 2366-2380, 1 Oct.-Dec. 2022, doi: 10.1109/TCC.2021.3051622.

[17] Y. Miao, Q. Huang, M. Xiao and H. Li, "Decentralized and Privacy-Preserving Public Auditing for Cloud Storage Based on Blockchain," in IEEE Access, vol. 8, pp. 139813-139826, 2020, doi: 10.1109/ACCESS.2020.3013153.

DoI: 10.63949/crinfo.v2i1.004