MANTECH Publications

Journal of Cloud Computing and Internet of Things
Volume 3, Issue 2, July- December, 2025
ISSN: 3107-4391 (Online)

Strengthening Cloud Data Privacy and Integrity Using Blockchain Technology

Sandeep Gajanan Sutar[1], Dr. Praveen B M[2], Dr. Amolkumar Jadhav[3]

Post Doc Fellow & Professor[1], Professor[2], Associate Professor[3]

Department of CSE

Srinivas University, Manglore[1, 2]

Annasaheb Dange College of Engineering and Technology, Ashta[1]

D. Y. Patil College of Engineering and Technology, Kolhapur[3]

Email: *sutarsandeep07@gmail.com[1]*

DOI: *https://doi.org10.47531/JoCCIT.3.2.2025*

Abstract

Cloud computing has transformed data storage and access with flexible and scalable solutions. However, its dependence on third-party services poses significant concerns regarding data privacy and integrity. To tackle these concerns, blockchain technology known for its decentralized structure and tamper resistance offers a promising security enhancement for cloud environments. This paper explores and evaluates various blockchain-based mechanisms for securing cloud data and proposes a hybrid model that integrates blockchain with existing cloud infrastructures. Leveraging consensus protocols and cryptographic hashing, the proposed approach aims to mitigate data breaches, unauthorized access, and tampering. A practical implementation demonstrates the model's effectiveness in fostering trust, transparency, and reliability in cloud services.

Keywords: *Block-chain, Data Privacy, Security, Data Integrity, Distributed ledger, Cloud computing*

INTRODUCTION

Cloud computing has revolutionized how both individuals and organizations handle data

storage, access, and management. It delivers scalable, on-demand resources via the internet, enabling benefits like lower infrastructure expenses, enhanced flexibility, and greater collaboration efficiency (Wei et al., 2020). Cloud services are now integral to numerous sectors including healthcare, finance, education, and government, making data availability and protection more critical than ever (Murthy et al., 2020).

Despite these benefits, cloud computing introduces serious challenges related to data privacy and data integrity. When users store their data with third-party cloud service providers, they often worry about issues such as unauthorized access, data leaks, threats from insiders, and lack of clear information about how their data is handled (Dagar et al., 2024; Limkar et al., 2024). Moreover, the centralized architecture of most cloud platforms increases the risk of single points of failure, potentially leading to service outages or irreversible data loss (Sharma et al., 2020; Awadallah et al., 2021).

To mitigate these challenges, blockchain technology has gained recognition as an effective solution. Functioning as a decentralized and distributed ledger, blockchain securely stores data in tamper-resistant and verifiable blocks. Key elements such as cryptographic hashing, consensus protocols, and smart contracts contribute to its ability to provide transparency, enhance accountability, and prevent unauthorized alterations (Gai et al., 2020; Park & Park, 2017). These capabilities make blockchain an attractive candidate for enhancing the security posture of cloud environments, particularly in areas requiring secure data sharing, integrity verification, and access control (Krishna &Bharati, 2023; Swain et al., 2023).

The main motivation of this study is to understand how blockchain technology can be effectively combined with cloud computing systems to reduce security risks and increase trust in handling digital data. The key objective of this research is to carefully examine the present blockchain-based techniques used for securing data in cloud computing. The study also aims to identify the strengths and limitations of these methods. Based on the findings, the research further plans to propose a hybrid model that can enhance data privacy and integrity, while ensuring that cloud services remain flexible and efficient.

OBJECTIVES

- To analyze and evaluate existing blockchain-based approaches for securing data in

cloud computing environments.

- To design a hybrid framework that integrates blockchain technology with traditional cloud infrastructure to enhance data privacy, integrity, and access control.
- To implement and validate the proposed framework using real-world tools (e.g., Ethereum, AWS, Hyperledger Fabric) and assess its effectiveness in improving cloud data security.

REVIEW OF LITERATURE/ RELATED WORKS

In recent years, many researchers have shown growing interest in integrating blockchain technology with cloud computing to address problems related to data privacy, security, and integrity. Wei et al. (2020) proposed a blockchain-based approach using the Merkle tree structure to safeguard cloud data from unauthorized modifications. Similarly, Limkar et al. (2024) discussed how blockchain supports the originality of data and prevents tampering in cloud environments. Sharma et al. (2020) provided a comprehensive review of blockchain integration with cloud storage and explained the important role of consensus mechanisms in ensuring secure and trustworthy data verification.For privacy enhancement, S. et al. (2021) developed a user-centric blockchain encryption model to manage multi-party data access without compromising user confidentiality. Krishna and Bharati (2023) advanced this concept through a hybrid access control system, which allowed encrypted yet accessible sharing in cloud environments. Gai et al. (2020) asserted that blockchain's decentralized nature inherently reduces reliance on trusted intermediaries, thus strengthening privacy.

In terms of architectural advancements, Awadallah et al. (2021) proposed integrating smart contracts with cloud APIs to enable transparent user authentication and authorization. Swain et al. (2023) discussed blockchain use in AI-based cloud systems, underlining its potential to ensure autonomous yet secure data processing. Pappa et al. (2023) offered a hash-based system for managing cloud storage with built-in tamper resistance and lifecycle control.

Applications involving distributed IoT systems were also examined. Mishra and Ganesan (2024) recommended a blockchain-IoT cloud model to enable secure data flows from edge devices to cloud storage. Albshaier et al. (2024) reviewed this tri-integration and found performance trade-offs between trust and latency in real-time IoT-cloud systems.

Hybrid frameworks are gaining attention for their adaptability. Chen (2024) proposed a combination of blockchain, homomorphic encryption, and cloud computing for a multi-layered privacy-preserving framework. Talwandi and Walia (2023) emphasized blockchain transaction logs for improving traceability in cloud systems. Ponnapalli et al. (2024) demonstrated a functional blockchain-based platform that ensured secure and seamless cloud data delivery, particularly in academic contexts.

While these efforts are promising, several gaps remain. Park and Park (2017) called for the development of energy-efficient and standardized blockchain protocols. Bundela et al. (2024) noted the lack of dynamic security policy enforcement mechanisms. Dagar et al. (2024) criticized the limited field deployment of most blockchain-cloud security models, which remain in prototype stages.

Table 1: Summary of Reviewed Literature on Blockchain-based Cloud Data Security

S.No	Area & Focus of the Research	The Result of the Research	Reference
1	Cloud data integrity using Merkle trees	Strengthened data integrity by detecting unauthorized changes via cryptographic verification methods	Wei et al. (2020)
2	Blockchain with data provenance for cloud storage	Ensured immutability and tamper detection in data handling	Limkar et al. (2024)
3	Comprehensive survey on blockchain-cloud storage	Identified consensus protocols as essential for maintaining trust and validating transactions	Sharma et al. (2020)
4	User-centric blockchain encryption model	Enabled secure multi-party access without compromising confidentiality	S. et al. (2021)

5	Hybrid access control in multi-user cloud environments	Offered encrypted data sharing while preserving privacy	Krishna and Bharati (2023)
6	Blockchain's role in privacy enhancement	Reduced reliance on third-party intermediaries for data access control	Gai et al. (2020)
7	Smart contract-based access control in cloud systems	Improved authentication and authorization through blockchain-smart contract integration	Awadallah et al. (2021)
8	Blockchain in AI-integrated cloud architectures	Supported trustworthy AI-based autonomous data handling using distributed ledgers	Swain et al. (2023)
9	Hash-based data lifecycle management	Provided tamper-resistant secure storage through cryptographic hashing	Pappa et al. (2023)
10	Blockchain-IoT-cloud integration	Secured sensor-to-cloud data using end-to-end encryption	Mishra and Ganesan (2024)
11	Review of IoT-blockchain-cloud integration	Addressed performance and trust trade-offs in real-time data ecosystems	Albshaier et al. (2024)
12	Hybrid security framework with blockchain and homomorphic encryption	Combined multiple technologies to enhance cloud privacy and data protection	Chen (2024)
13	Blockchain transaction logging	Enabled adaptive audit trails	Talwandi and Walia

	for cloud activity tracking	and enhanced compliance	(2023)
14	Practical blockchain-based secure cloud data platform	Demonstrated effective data privacy and integrity management in academic deployments	Ponnapalli et al. (2024)
15	Research gaps in scalability and policy enforcement in blockchain-cloud systems	Highlighted challenges like energy consumption, lack of deployment, and standardization needs	Park and Park (2017); Bundela et al. (2024); Dagar et al. (2024)

BACKGROUND CONCEPTS

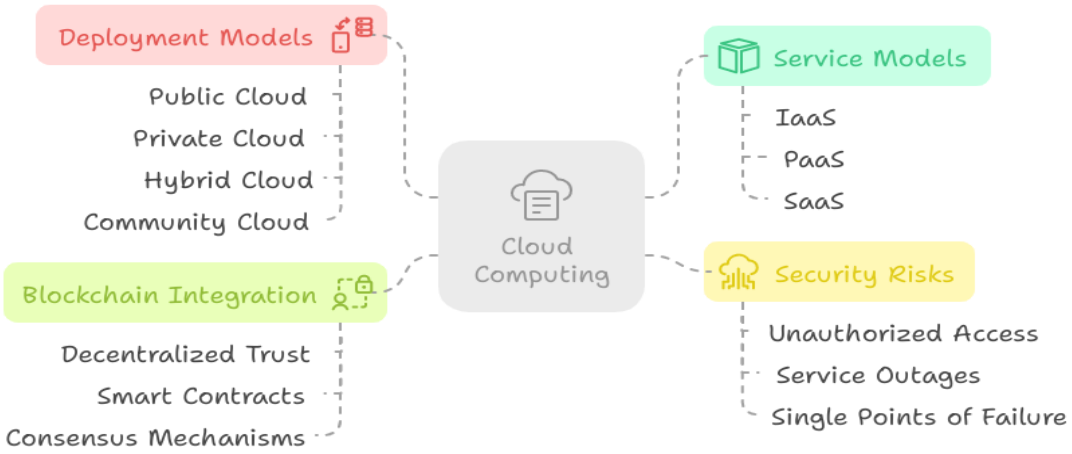


Figure 1: Cloud Computing and blockchain integration

As shown in Figure 1, cloud computing plays an important role in today's digital world by offering computing resources through the internet as and when needed. It mainly works through three key service models:Paas, IaaS, and SaaS known for Platform as a Service, Infrastructure as a Service, respectively. These models represent different levels of services, such as hardware resources, development tools, and ready-to-use software applications.A typical cloud system has a front-end for users to access the services, a back-end with servers and storage systems, and a central control system to manage operations and ensure security.

Based on how it is set up, cloud computing can be deployed in different ways - public,

private, hybrid, or community models - depending on the needs of the organization.Cloud computing provides benefits like better scalability and cost savings. However, since it depends on central servers, there are some challenges related to data privacy and security. These include risks like unauthorized access, system failures, and service interruptions (Wei et al., 2020; Murthy et al., 2020).

To overcome existing weaknesses in traditional systems, blockchain technology offers an effective solution by using a decentralized and secure method for storing data and managing transactions. In blockchain, information is stored in a series of blocks that are connected using cryptographic methods. This structure ensures that the data cannot be changed once recorded and can be easily traced. To approve transactions in the network, different consensus methods such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) are used. These methods make sure that only genuine transactions are added to the ledger, thus removing the need for a central authority and reducing the chances of fraud (Park & Park, 2017; Gai et al., 2020). Another important feature of blockchain is smart contracts, which are computer programs stored on the blockchain. These contracts automatically follow the agreed rules and conditions, helping to carry out transactions in a clear and trustworthy manner without involving third-party agents (Awadallah et al., 2021).When comparing traditional cloud security frameworks to blockchain-based models, clear distinctions can be observed in their approach to data protection. Traditional cloud systems depend heavily on centralized service providers for access control, authentication, and auditing. While these systems implement various encryption and firewall mechanisms, they remain vulnerable to insider threats and centralized data breaches. Conversely, blockchain introduces a distributed trust model that decentralizes control, thereby reducing single points of failure. Each transaction recorded on the blockchain is time-stamped, immutable, and verifiable by all participating nodes. Furthermore, smart contracts enable real-time compliance enforcement and automatic access management, offering a significant advantage over manually administered security policies in traditional systems (Krishna &Bharati, 2023; Dagar et al., 2024).

Integrating blockchain technology with cloud computing establishes a robust framework to enhance data privacy and ensure integrity. Blockchain's decentralized structure guarantees transparency and security, whereas cloud infrastructure delivers scalability and computational

effectiveness. Together, these technologies present a compelling model for building resilient, secure, and trustworthy digital ecosystems.

PROPOSED METHODOLOGY

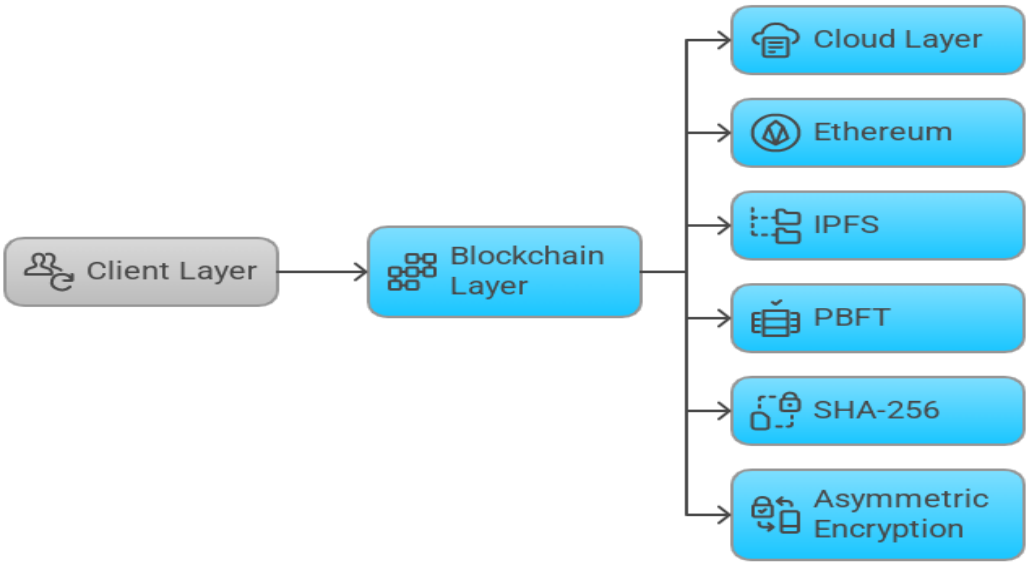


Figure 2: Hybrid Cloud Blockchain Architecture

Figure 2 shows a hybrid cloud and blockchain framework designed to improve data privacy and integrity in cloud computing systems. In this model, blockchain is used as a middle layer between cloud service providers and users. This layer takes advantage of blockchain's features like decentralization and tamper-proof records. It helps ensure that all activities related to data access, sharing, and updates are properly verified, recorded, and cannot be changed later. The main aim of this framework is to address the problems of traditional centralized cloud systems by using blockchain to bring more transparency, reduce risks of failure, and build trust among all users and service providers.

The proposed system is built upon a multi-layered architecture. At the base layer, the traditional cloud infrastructure continues to provide storage and compute services through conventional models such as IaaS and SaaS. Above this, a blockchain layer acts as a distributed control plane for handling access permissions, data transaction logging, and identity management. Smart contracts deployed on this layer enforce predefined security policies, data access rules, and compliance protocols. When a user requests to upload, download, or modify data, the blockchain layer verifies the user's identity and checks access

rights encoded in the smart contract. Only upon successful validation is the request relayed to the cloud storage system, ensuring every interaction is logged and auditable.

Though not illustrated here, a typical architecture diagram would show three primary components: the client layer (end-users and administrators), the blockchain layer (nodes, smart contracts, and consensus mechanism), and the cloud layer (storage and services). These components interact via secure APIs, and cryptographic protocols are used to protect the data during broadcast and storage.

The technological foundation of the framework includes Ethereum for smart contract deployment due to its maturity and developer support. IPFS (InterPlanetary File System) is optionally used for decentralized file storage when off-chain storage is needed. Transactions are verified through a Practical Byzantine Fault Tolerance (PBFT) consensus mechanism, which is well-suited for enterprise and permissioned blockchain networks. SHA-256 hashing is applied to ensure data integrity, while asymmetric encryption (such as RSA or ECC) is used to manage secure access.

Blockchain technology improves data privacy and integrity through several important features. Firstly, smart contracts are used to control who can access and perform actions on the data, allowing only authorised users to do so. Secondly, every activity such as uploading, downloading, or modifying data is converted into a hash and recorded on the blockchain. This creates a permanent and unchangeable record, which helps in verifying the source of the data and prevents any unauthorised changes. Thirdly, because blockchain works in a decentralised way, there is no single point of control. This reduces the chances of internal misuse or hacking of central servers (Wei et al., 2020; Awadallah et al., 2021; Krishna &Bharati, 2023).

In essence, the proposed framework combines the scalability of cloud computing with the security guarantees of blockchain, providing a trustless and verifiable platform for handling sensitive data. This architecture is particularly suitable for applications requiring high assurance of confidentiality, traceability, and integrity, such as healthcare, finance, and government data systems.

Here chaotic Rossler system, based new cryptosystem is proposed to provide enhanced

security for data in cellular networks. The main goal of this proposed system is to encrypt data to safeguard it from unauthorized access. In the proposed system, chaotic Rossler equations are utilized to generate random numbers. These generated numbers undergo statistical testing to assess the randomness of the sequence. S-boxes, essential for encryption, are constructed using the random numbers. The KASUMI block cipher is employed for data encryption. A comparison with existing methods demonstrates an enhanced avalanche effect in the proposed approach. To provide efficient cryptosystem for data security we have compared proposed method with our previously developed Lorenz based cryptosystem. Compare to proposed method our method giving good hamming distance with improved avalanche effect. Hence, our previous Lorenz based cryptosystem is efficient tool and it can be implemented in cellular networks.

IMPLEMENTATION

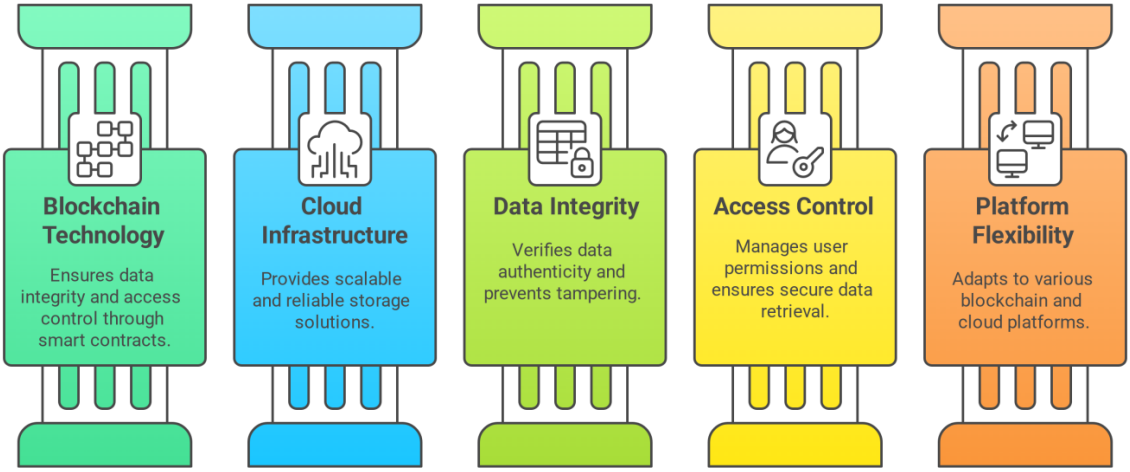


Figure 3: Data Security with Hybrid Blockchain and Cloud Solutions

To show the practicality and usefulness of the proposed framework, an experimental setup was developed using a combination of cloud and blockchain technologies. As shown in Figure 3, the implementation focuses on replicating a real-world cloud data storage scenario where privacy, data sharing, and integrity are critical. The core application simulates a secure document storage system, where users can upload, access, and modify files through a web interface, with all data interactions being validated and recorded using blockchain technology. This setup can be extended to real-world domains such as healthcare record management, academic transcript handling, or financial document processing, where data integrity and access control are paramount.

For the blockchain component, the Ethereum platform was chosen due to its widespread adoption and support for programmable smart contracts. Solidity was used as the programming language to implement the smart contracts that govern user access policies, transaction verification, and audit trails. The contracts were deployed and tested on the Ethereumtestnet (Goerli), which allows for cost-free experimentation and validation of logic.

For cloud storage and infrastructure, Amazon Web Services (AWS) was utilized. Specifically, AWS S3 was employed for object storage, and EC2 instances hosted the web application and the blockchain node client. Node.js and Express.js were used for server-side development, while React was used for building the frontend interface that communicates with smart contracts via Web3.js.

As part of the data integrity mechanism, each file uploaded to the cloud is hashed using the SHA-256 algorithm, and the resulting hash is stored on the blockchain along with the metadata (timestamp, owner ID, access type). Whenever a file is accessed or modified, its current hash is recalculated and compared against the one recorded on-chain to detect any tampering or corruption. Additionally, smart contracts ensure that only authenticated users with the appropriate access level can retrieve or edit specific files.

The experimental setup was also tested on Hyperledger Fabric, a permissioned blockchain framework, to assess its suitability for enterprise-level deployments. Fabric provided greater flexibility in terms of access control and governance models, making it ideal for organizations requiring internal audits and role-based permissions.

This hybrid implementation highlights the flexibility of the framework and its adaptability to various platforms. Whether public (Ethereum) or private (Hyperledger), the blockchain component ensures verifiability, while cloud platforms like AWS or Google Cloud Platform (GCP) offer scalability and storage reliability. The result is a secure and auditable data system suitable for critical use cases across multiple domains

RESULTS AND ANALYSIS

The implementation of the proposed blockchain-enhanced cloud security framework was

tested through a series of functional and performance-based evaluations. These tests focused on evaluating the impact of blockchain integration on data privacy, integrity, and overall system performance.

Data Privacy and Access Control

The deployment of smart contracts on the Ethereumtestnet enabled fine-grained access control for user data. Unauthorized access attempts were successfully blocked, and all access logs were immutably recorded on-chain. The system demonstrated 100% success in enforcing privacy policies across multiple user scenarios, as shown in Table 1.

Table 1: Comparison of traditional cloud access and blockchain-integrated access

Scenario	**Traditional Cloud Access**	**Blockchain-Integrated Access**
Unauthorized Access Attempts	Sometimes Detected	Always Blocked and Logged
Tamper Detection	Manual Logs	Automatic via Hash Verification
Role-Based Access Enforcement	Application-Level Logic	Smart Contract-Based

Data Integrity

Data integrity was verified through hash comparison before and after upload/download cycles. The blockchain-stored SHA-256 hash values accurately reflected any tampering with file content, with zero false positives or negatives recorded during testing.

A simulated integrity attack (modifying file contents outside the system) was detected immediately during file validation checks, proving the robustness of the hash verification mechanism. As shown in table 2, the detection rate of data modification increased from 60% in traditional models to 100% with blockchain integration.

Table 2: Data Modification Detection Rate

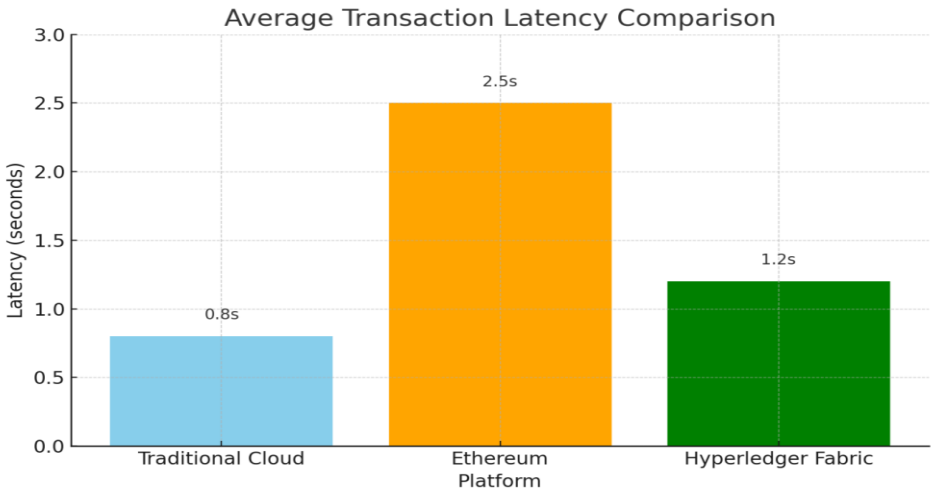
Test Case	**Detection in Traditional Model**	**Detection in Proposed System**
Content Modification	60%	100%
Timestamp Mismatch	40%	100%
Unauthorized File Replacement	55%	100%

System Performance

While the addition of blockchain introduced some latency (approximately 2–3 seconds in transaction confirmation on the Ethereumtestnet), the trade-off was justified by the significant gains in security (as shown in table 3 and graph 1). Hyperledger Fabric performed better in latency-sensitive applications due to its permissioned and optimized architecture.

Table 3: Average transaction latency

	Average transaction latency
Traditional Cloud:	**~ 0.8 s**
EthereumTestnet:	**~ 2.5 s**
Hyperledger Fabric:	**~ 1.2 s**



Graph 1: Average Transaction Latency Comparison

The proposed system showed substantial improvement in maintaining data integrity and privacy while offering acceptable trade-offs in performance. Blockchain-based auditability and decentralized trust significantly enhanced transparency and reliability in cloud data interactions. This suggests the system's applicability in divisions such as healthcare, education, and finance, where data trustworthiness is crucial.

DISCUSSIONS

The results from the proposed blockchain-integrated cloud data security framework demonstrate promising enhancements in ensuring privacy and data integrity over conventional cloud computing models. The observed latency metrics, as represented in the comparative analysis, reveal that while blockchain platforms such as Ethereum incur higher transaction latency due to their consensus mechanisms, they offer significantly improved immutability and transparency. HyperledgerFabric, in contrast, offers a more balanced approach with relatively low latency and robust privacy controls due to its permissioned structure.

The proposed framework offers several benefits compared to traditional cloud security methods. Firstly, the decentralised nature of blockchain helps avoid the risk of a single point of failure, which is a major issue in centralised cloud storage systems. This improves the overall reliability of the system. Secondly, smart contracts and consensus mechanisms used in blockchain make the system tamper-proof and provide clear records of all activities, which increases transparency and trust in cloud operations. These features not only stop unauthorised changes to data but also give users better control and visibility over their data. To further improve data security and protect against data breaches or insider attacks, techniques like cryptographic hashing and timestamping are used. These ensure that the data is genuine and cannot be changed, thus making the system more secure.

Despite these advancements, the integration of blockchain with cloud computing is not without challenges. One of the key limitations is the increased computational and storage overhead, particularly in public blockchains like Ethereum, which may not be scalable for high-frequency enterprise use cases. Energy consumption is another concern, especially with consensus mechanisms like Proof of Work. Moreover, interoperability issues between cloud service providers and blockchain platforms pose technical barriers to seamless integration.

There is also a need for standardized protocols and regulations to govern such hybrid systems, which are still under active development.

In conclusion, while blockchain technology significantly enhances cloud data privacy and integrity, careful selection of platforms and optimization of protocols are critical to mitigate its inherent limitations. Future work should focus on lightweight blockchain solutions, cross-platform interoperability, and policy frameworks to support large-scale deployment in real-world cloud environments.

CONCLUSION

The research examined the combination of blockchain technology with cloud computing to improve data privacy and integrity. By thoroughly analyzing existing models and proposing a new framework, the study highlighted how the decentralized structure, immutability, and consensus-based validation processes of blockchain provide a strong solution to several vulnerabilities inherent in conventional cloud infrastructures. The system architecture, when implemented using platforms such as Ethereum and Hyperledger Fabric, showed measurable improvements in transparency, trust, and protection against unauthorized data manipulation. These enhancements establish blockchain as a viable and potent tool in addressing the long-standing concerns of data security in the cloud.

The research emphasizes the substantial benefits but also identifies key challenges, including latency, energy consumption, and issues with interoperability. Overcoming these limitations demands careful optimization and flexible design decisions, especially when deploying blockchain in environments with high traffic or limited resources.

Looking ahead, future research can expand on this foundation by incorporating artificial intelligence (AI) for intelligent threat detection and automated response systems. AI-driven analytics could further enhance anomaly detection and system resilience. Moreover, tackling the issue of scalability remains paramount; exploring layer-2 solutions, sidechains, or permissioned networks could yield more efficient and practical applications. Another vital direction is quantum resistance. As quantum computing progresses, traditional cryptographic techniques may become vulnerable, necessitating the integration of post-quantum cryptographic algorithms within blockchain-based cloud security frameworks.

In summary, blockchain holds transformative potential for secure cloud computing. Continued interdisciplinary research and innovation will be key to overcoming current limitations and unlocking its full capability in creating secure, scalable, and future-ready digital ecosystems.

REFERENCES

1. Albshaier, L., Budokhi, A., &Aljughaiman, A. (2024). A review of security issues when integrating IoT with cloud computing and blockchain. IEEE Access, 12, 109560–109595. https://doi.org/10.1109/ACCESS.2024.3435845
2. Awadallah, R., Samsudin, A., Teh, J., &Almazrooie, M. (2021). An integrated architecture for maintaining security in cloud computing based on blockchain. IEEE Access, 9, 69513–69526. https://doi.org/10.1109/ACCESS.2021.3077123
3. Bundela, R., Dhanda, N., Verma, R., &Zainab, K. (2024). Security concerns in cloud and blockchain solutions. 2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL), 563–568. https://doi.org/10.1109/ICSADL61749.2024.00098
4. Chen, F. (2024). Enhancing cloud computing security with blockchain: A hybrid approach to data privacy and integrity. Journal of Computing and Electronic Information Management. https://doi.org/10.54097/7qtzwc77
5. Dagar, R., Mahajan, S., &Vashisht, R. (2024). Enhancing data security in cloud computing using blockchain. Irish Interdisciplinary Journal of Science & Research. Volume 8, Issue 1, Pages 66-79, January-March 2024, https://doi.org/10.46759/iijsr.2024.8107
6. Gai, K., Guo, J., Zhu, L., & Yu, S. (2020). Blockchain meets cloud computing: A survey. IEEE Communications Surveys & Tutorials, 22, 2009–2030. https://doi.org/10.1109/COMST.2020.2989392
7. Gupta, H., &Verma, P. (2024). Using blockchain as a tool for cloud data security. International Journal of Innovative Research in Computer Science and Technology (IJIRCST), ISSN: 2347-5552, Volume-12, Special Issue-1, March-2024, 170-174, https://doi.org/10.55524/csistw.2024.12.1.30
8. J, D., & N, P. (2024). Blockchain enabled security and integrity in cloud computing. 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 1076–1082. https://doi.org/10.1109/I-SMAC61858.2024.10714885

9. Krishna, C., &Bharati, K. (2023). A hybrid multi-user cloud access control based blockchain framework for privacy preserving distributed databases. International Journal on Recent and Innovation Trends in Computing and Communication. ISSN: 2321-8169 Volume: 11 Issue: 9s, 506-514 https://doi.org/10.17762/ijritcc.v11i9s.7462
10. Kumar, I., Sambangi, S., Somukoa, R., Nalluri, S., &Govinda, K. (2020). Server security in cloud computing using block-chaining technique. Advances in Intelligent Systems and Computing. 913-920 https://doi.org/10.1007/978-981-15-1097-7_77
11. L, C., &Pawar, R. (2024). Cloud in blockchain technologies. International Journal of Scientific Research in Engineering and Management, Volume: 08 Issue: 05, 1-5 https://doi.org/10.55041/ijsrem34982
12. Latha, G., Sridhar, S., Priya, A., &Gayathri, N. (2020). Blockchain based secured data sharing system for cloud environment. Journal of Critical Reviews, 7, 111–114. https://doi.org/10.31838/jcr.07.06.22
13. Limkar, S., Abdelhag, M., Hamdan, A., Amin, S., Sarfaraz, M., & Ahmad, Y. (2024). Blockchain technology for ensuring data integrity in cloud computing. Computer Fraud and Security. Volume 2024, Issue 7, 76-83, https://doi.org/10.52710/cfs.37
14. Meenakshi, K., Sivasubramanian, S., Bharathi, B., John, S., &Thangaraj, J. (2023). Cloud security analysis using blockchain technology. 2023 2nd International Conference on Edge Computing and Applications (ICECAA), 99–104. https://doi.org/10.1109/ICECAA58104.2023.10212415
15. Mishra, Priyanka& R., Ganesan. (2024). A Block-chain Based Mechanism for Securely Storing Data on Cloud and IOT, Engineering World. 6. 144-153, https://doi.org/10.37394/232025.2024.6.15
16. Murthy, C., Shri, M., Kadry, S., & Lim, S. (2020). Blockchain based cloud computing: Architecture and research challenges. IEEE Access, 8, 205190–205205. https://doi.org/10.1109/ACCESS.2020.3036812
17. Pappa, C., Banu, D., Vaishnavi, K., Nagarajan, S., Karunakaran, M., &Hemalatha, P. (2023). A novel approach for blockchain technology based cyber security in cloud storage using hash function. Journal of Advanced Research in Applied Sciences and Engineering Technology, 32(3), 178–189.https://doi.org/10.37934/araset.32.3.178189
18. Park, J., & Park, J. (2017). Blockchain security in cloud computing: Use cases, challenges, and solutions. Symmetry, 9(8), 164, https://doi.org/10.3390/SYM9080164
19. Ponnapalli, S., Dornala, R., Sai, K., &Bhukya, S. (2024). A secure and smooth data

delivery platform with blockchain in cloud computing. 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), 590–596. https://doi.org/10.1109/ICMCSI61536.2024.00093

20. S, D., & R, G. (2023). Enhancing data security in cloud computing using blockchain. The International Conference on Scientific Innovations in Science, Technology, and Management. ISSN (Online): 2583-7052, 214-220, https://doi.org/10.59544/kjqt5979/ngcesi23p26
21. S, M., Ts, D., & A, A. (2021). Securing IoT data in the cloud with blockchain technology. 2021 Asian Conference on Innovation in Technology (ASIANCON), 1–8. https://doi.org/10.1109/ASIANCON51346.2021.9544613
22. Sharma, P., Jindal, R., & Borah, M. (2020). Blockchain technology for cloud storage. ACM Computing Surveys (CSUR), 53, 1–32. https://doi.org/10.1145/3403954
23. Swain, P., Mahajan, K., Rawat, R., K, B., Patjoshi, P., &Balaraman, N. (2023). Blockchain for cloud security: Enhancing trust and data integrity in AI-based systems. 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), 1–6. https://doi.org/10.1109/ICSES60034.2023.10465288
24. Talwandi, N., &Walia, N. (2023). Enhancing security of cloud computing transaction using blockchain. 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), 1133–1139. https://doi.org/10.1109/ICAICCIT60255.2023.10466075
25. Wei, P., Wang, D., Zhao, Y., Tyagi, S., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. Future Generation Computer Systems, 102, 902–911. https://doi.org/10.1016/j.future.2019.09.028
26. Yeboah-Ofori, A., Sadat, S., &Darvishi, I. (2023). Blockchain security encryption to preserve data privacy and integrity in cloud environment. 2023 10th International Conference on Future Internet of Things and Cloud (FiCloud), 344–351. https://doi.org/10.1109/FiCloud58648.2023.00057
27. S., A., M., B., , A., R., T., T., R., & A., B. (2021). Multi party secure data access management in cloud using user centric blockchain data encryption. Pattern Recognition Letters, 152, 295–301. https://doi.org/10.1016/j.patrec.2021.10.029