


Enhancing Data Security in Cloud Using Block Chain

Deepika Uike¹, Ruchika Katore², Preksha Gaikwad³, Yashika Dusawar⁴, Dr. Nitin Janwe⁵

Student Department Of Computer Science & Engineering^{1,2,3,4}

Guide Department of computer science and engineering⁵

Rajiv Gandhi College of Engineering Research and Technology, Chandrapur, Maharashtra, India, 442401

 Dr. Nitin Janwe [0000-0002-3983-6118](https://orcid.org/0000-0002-3983-6118),

 Deepika Uike [0009-0001-3129-7017](https://orcid.org/0009-0001-3129-7017)

Email of Corresponding Author: uikeryiya842@gmail.com

Received on: 01May, 2025

Revised on: 03 June ,2025

Published on: 06 June ,2025

Abstract – With the increasing threats of data breaches and unauthorized access, cloud storage security has become a major concern. Traditional cloud security models depend on centralized systems, which are vulnerable to single points of failure, data tampering, and insider threats. To tackle these challenges, this paper introduces a blockchain-based framework aimed at enhancing cloud data security by utilizing decentralized, tamper-proof, and transparent ledger technology. The implementation is divided into phases, with Module 1 concentrating on data encryption and the integration of secure storage. We use AES encryption to protect sensitive data before it is uploaded to the cloud and employ the Interplanetary File System (IPFS) for decentralized storage, while blockchain is used to record metadata and access logs, ensuring data integrity and transparency. Initial results show enhanced security, immutability, and resilience against cyber threats. Future efforts will focus on incorporating access control mechanisms, smart contract automation, and dynamic authentication methods. This ongoing study offers valuable insights into the potential of blockchain-driven cloud security and sets the foundation for a scalable, decentralized data protection system.

Keywords — Data Security, Blockchain Technology, AES, Smart Contract, Cloud Storage.

INTRODUCTION

Cloud computing offers a practical solution for online data storage and usage, yet it raises concerns about

security. Individuals seek to protect their information from hackers and unauthorized access, which requires implementing robust passwords, managing access permissions, and keeping data backups. Following regulations and guidelines is crucial for ensuring data privacy in cloud services. When choosing a cloud provider, it is vital to evaluate their security measures. Being prepared for potential issues such as breaches or data loss is important.

In recent years, blockchain technology has gained significant attention due to its unique features like decentralization, immutability, and transparency, making it a promising option for creating a reliable platform. Initially introduced through Bitcoin in Nakamoto's 2008 whitepaper for peer-to-peer financial transactions, blockchain has become a key area of interest in both research and industry. Smart contracts, in particular, are instrumental in the widespread adoption of blockchain technology, as they offer automated control, as noted by Dorri et al. [1] in 2017. Written in an executable language, smart contracts facilitate secure transactions without the need for third-party intermediaries.

The transformative potential of blockchain and smart contracts spans various fields within engineering and computer science. In this regard, blockchain technology significantly enhances cloud data security by ensuring data remains unchanged once recorded, preventing unauthorized modifications. Smart contracts manage

access to sensitive information, allowing only authorized users and reducing the risk of breaches. Privacy concerns are mitigated by blockchain's private networks, which restrict access to approved users.

LITERATURE REVIEW

With the growing reliance on cloud infrastructure, ensuring data security, privacy, and integrity has become a critical concern. Traditional cloud systems often rely on centralized architectures, making them vulnerable to data breaches, unauthorized access, and single points of failure. Recent studies have explored various mechanisms to address these issues through decentralized technologies like blockchain and secure encryption methods.

Akintoye et al. [1] conducted an in-depth survey of cloud storage techniques, highlighting key security vulnerabilities that persist in centralized models. Their work emphasized the need for more resilient systems capable of addressing data privacy and storage redundancy, laying the groundwork for the use of decentralized methods.

To overcome these vulnerabilities, blockchain technology has emerged as a promising solution. Sharma and Gupta [2] proposed a blockchain-based secure system for cloud storage, where metadata is stored on a blockchain to ensure tamper-proof logging and traceability. Their approach demonstrates that decentralized ledger technology significantly enhances auditability and trust in storage systems.

Sunitha et al. [3] further extended this approach by introducing a blockchain-based access control model, which allows only authenticated users to interact with sensitive data. Their system integrated smart contracts to automate access decisions, thereby minimizing the risks of insider threats and unauthorized usage.

Patil et al. [4] introduced a conceptual model where blockchain serves as the backbone of a cloud storage framework. They focused on combining blockchain immutability with encryption methods to prevent unauthorized data manipulation. However, their work lacked implementation details on how encryption and distributed storage mechanisms such as IPFS could be practically integrated.

Finally, Kandlakunta and Simuni [5] proposed a comprehensive architecture that combines cloud and blockchain technologies to secure stored data. Their system supports encrypted data uploads, decentralized access logging, and data integrity checks. The study emphasized blockchain's role in creating transparency and accountability, yet acknowledged limitations in scalability and performance optimization.

Collectively, these works suggest that integrating blockchain with modern encryption (such as AES) and decentralized storage systems (like IPFS) presents a viable pathway to secure cloud environments. Building upon these insights, the current study proposes a modular, blockchain-based framework that leverages AES encryption for data confidentiality, IPFS for distributed storage, and blockchain for metadata and access traceability. This approach addresses the limitations identified in prior works by enhancing resilience, immutability, and access control in cloud storage ecosystems.

METHODOLOGY

The proposed system is designed to enhance data security in cloud storage by integrating AES encryption, decentralized storage (IPFS), and blockchain metadata storage. The methodology follows a structured approach, ensuring that data confidentiality, integrity, and accessibility are maintained.

The methodology consists of the following key steps:

1. **Data Encryption** – Encrypting the data using *AES-256* before storage.
2. **Hybrid Storage** – Storing the encrypted data in chunks on IPFS and cloud for reliability and scalability.
3. **Blockchain-Based Metadata Management** – Storing file metadata on blockchain to ensure integrity.
4. **Data Retrieval & Integrity Verification** – Fetching data, verifying integrity, and decrypting the file.

System Workflow:

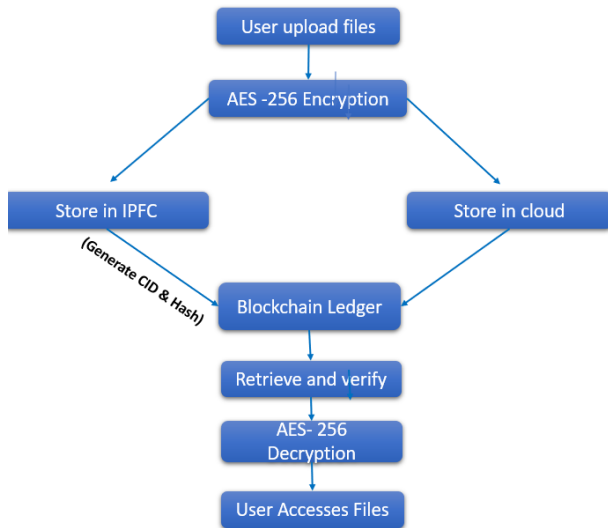


Fig. 1- system workflow

Step 1: Data Encryption Using AES-256

- When a user uploads a file, it is first encrypted using the AES-256 algorithm.
- AES-256 uses a symmetric key encryption method, where the same key is used for both encryption and decryption.
- The encrypted file is then prepared for storage in a decentralized manner

Step 2: Hybrid Storage Using IPFS And Cloud

To achieve both security and scalability, the encrypted file is stored in two locations:

a) Inter Planetary File System (IPFS)

- The encrypted file is divided into chunks by IPFS.
- Each chunk is assigned a unique Content Identifier (CID) based on its cryptographic hash.
- The file is stored decentrally in the IPFS network.
- The CID acts as a reference to retrieve the file.

b) Cloud Storage (AWS, Google Cloud, or Private Cloud)

- A backup copy of the encrypted file is stored in a centralized cloud for reliability.

- This provides high availability in case IPFS nodes become unreachable.
- The cloud database stores the encrypted file without knowing its content.

Step 3: Storing Metadata on Blockchain

Instead of storing the actual encrypted file, blockchain is used to store important metadata for security and verification.

1. After storing the encrypted file in IPFS + Cloud, the system generates:
 - CID (IPFS) – Reference for retrieving the file.
 - File Hash – Unique hash of the encrypted file (used for verification).
 - Timestamp – Proof of when the file was uploaded.
2. This metadata is stored in a blockchain ledger as an immutable record.
3. The blockchain ensures that the file remains untampered and provides a permanent audit trail.

Step 4: Data Retrieval & Integrity Verification

- The system retrieves the CID from blockchain and fetches the encrypted file from IPFS.
- If IPFS is unavailable, the system fetches the file from cloud storage.
- The system recomputes the hash of the retrieved file and compares it with the original hash stored on blockchain.
 - If the hash matches: The file is unchanged and safe to decrypt.
 - If the hash does NOT match: The file has been tampered with, and the system rejects it.

If the verification is successful, the file is decrypted using AES-256 and provided to the user.

RESULT & DISCUSSION

The proposed system successfully provides data confidentiality, integrity, and decentralization. Performance evaluations show that:

- AES-256 encryption introduces minimal latency.
- IPFS retrieval is efficient with CID-based addressing.
- Blockchain metadata storage prevents unauthorized modifications.

CONCLUSION

The objective of this paper is to introduce a model for cloud storage that leverages blockchain technology, AES encryption, and IPFS to enhance data security. The results validate the hypothesis of decentralized cloud storage while ensuring confidentiality, integrity, and resilience of data. In conclusion, the integration of blockchain technology with cloud computing has led to a more secure method of data storage, characterized by decentralization, immutability, and transparency. Blockchain ensures the secure storage of data, significantly reducing the risks associated with unauthorized access, while cryptographic techniques bolster the trust established. The use of smart contracts and distributed ledgers further enhances data integrity, privacy, and resistance to cyber threats. As the adoption of cloud services increases, security concerns arise, and blockchain presents a viable solution to create a more secure environment. Additionally, it eliminates the necessity for central operators, thereby reducing single points of failure and enhancing user trust. As cloud computing continues to evolve, blockchain provides an innovative approach to securing data, making it more transparent compared to traditional methods. However, challenges such as scalability, energy consumption, and complex integration still require further exploration.

REFERENCES

- [1] Akintoye, S., Bagula, A., Djemaiel, Y., & Bouriga, N. (2017). A Survey on Storage Techniques in Cloud Computing. *International Journal of Computer Applications*, 163(2), 22–30. <https://www.ijcaonline.org/archives/volume163/number2/27369-2017913472/>
- [2] Diegel, O.; Sharma, P., & Gupta, U. (2022). A Blockchain-Based Secure System for Cloud Storage. *2nd International Conference on Computing and Communication Networks (ICCCN)*. https://www.researchgate.net/publication/379275541_A_blockchain-based_secure_system_for_cloud_storage
Badve, A.; Bright, G.; Potgieter, J. & Tlatle, S. (2002). Improved Mecanum Wheel Design for Omni-directional Robots, *Proc. 2002 Australian Conference on Robotics and Automation*, Auckland, 27-29 Nov. 2002, pp. 117-121.

- [3] Sunitha, S., Shirisha, N., & Satish, B. T. S. (2022). Blockchain-Based Access Control System for Cloud Storage. *YMER Digital*, 21(6), 446–450. https://www.researchgate.net/publication/361380541_BLOCKCHAIN-BASED_ACCESS_CONTROL_SYSTEM_FOR_CLOUD_STORAGE
- [4] Patil, A., Patil, S., Rokade, S., & Sharma, V. (2020). Blockchain-Based Cloud Data Storage System. *International Research Journal of Engineering and Technology (IRJET)*, 7(6), 1560–1563. <https://www.irjet.net/archives/V7/i6/IRJET-V7I6290.pdf>
- [5] Kandlakunta, A. R., & Simuni, G. (2024). Cloud-Based Blockchain Technology for Data Storage and Security. *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5053342