International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

A Secure Storage Management Technique for Cloud in Collaborative Environment

Dr. Rajashree Shettar[1], Sai Ankit Panda[2], Prince Anshumaan[3]
[1,2,3]*Dept. of CSE, RV College of Engineering Bengaluru, India*

***Abstract*—This paper presents a secure storage management technique for cloud environments operating in collaborative settings. The proposed approach integrates blockchain technology with cloud storage to enhance data confidentiality, integrity, and access control. Data owners upload encrypted files to the cloud while file location information is recorded immutably on the blockchain. Only authorized users possessing valid decryption credentials can retrieve and access the stored data through searchable encryption and controlled key distribution. The sys-tem employs hashing for integrity verification, aggregate keys for efficient decryption, and periodic key rotation to strengthen security. Auditing and network monitoring further reduce vul-nerabilities and enable detection of anomalies. The proposed framework improves resistance to data breaches, unauthorized access, and malicious modification while maintaining usability and performance for large-scale cloud storage systems.**

***Index Terms*—blockchain, cloud storage security, secure data sharing, access control, cryptography, hashing, searchable en-cryption**

I. Introduction

In recent years, the rapid growth of data generated by organizations and users across the globe has created a strong demand for scalable and reliable storage solutions. Cloud computing has emerged as a dominant paradigm by offering on-demand storage, ubiquitous access, and reduced infrastruc-ture management. However, despite these advantages, cloud storage environments face critical challenges related to data privacy, integrity, trust, and control.

Traditional cloud storage systems rely on third-party ser-vice providers, which introduces risks such as data breaches, unauthorized access, lack of transparency, and potential single points of failure. Users often lose control over their data once it is outsourced to the cloud, raising concerns regarding data exposure, copyright issues, and malicious attacks.

To address these limitations, this paper proposes a secure storage management technique that integrates blockchain tech-nology with cloud storage in a collaborative environment.

Blockchain provides a decentralized and tamper-resistant ledger, ensuring immutability, transparency, and trust without depending on a centralized authority. In the proposed system, data owners upload encrypted files to the cloud, while only metadata such as file location is stored on the blockchain. Ac-cess to data is controlled through cryptographic mechanisms, aggregate keys, and searchable encryption, enabling only au-thorized users to retrieve and decrypt the stored content.

The proposed framework enhances data confidentiality, in-tegrity verification, and secure access control while support-ing efficient storage and retrieval operations. By combining blockchain with cloud computing, the system mitigates com-mon security threats and strengthens user confidence in cloud-based storage services.

II. Objectives

A. Primary Objective

To design and implement a secure blockchain-based cloud storage management system that enhances data privacy, in-tegrity, and controlled access in a collaborative cloud envi-ronment while preventing unauthorized data manipulation and breaches.

B. Secondary Objectives

1) To store encrypted data in the cloud while recording file location and related metadata on the blockchain to ensure transparency and immutability.
2) To apply Hierarchical Attribute-Based Encryption (HASBE) for fine-grained and scalable access control among multiple users.
3) To ensure that only authorized users possessing valid aggregate or secret keys are able to retrieve and decrypt cloud-stored data.
4) To employ the BLAKE2 cryptographic hashing algo-rithm to verify data integrity and prevent tampering.
5) To implement searchable encryption using trapdoor keys, enabling secure and efficient file search and re-trieval.
6) To minimize reliance on untrusted third-party stor-age providers by leveraging a decentralized blockchain ledger for trust management.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

7) To integrate auditing and monitoring mechanisms for de-tecting anomalies and improving overall system security.
8) To evaluate the performance of the proposed system in terms of security, efficiency, and storage management capability.

III. Methodology

The proposed methodology integrates blockchain technol-ogy with cloud storage to ensure secure data management in a collaborative environment. Data is encrypted by the data owner before being outsourced to the cloud, while only file metadata and hash values are stored on the blockchain to maintain transparency and immutability. Authorized users perform searchable encryption to locate files and use secret or aggregate keys for decryption and access. BLAKE2 hashing is employed for integrity verification, and key rotation is used to enhance security over time. The methodology also includes auditing and monitoring components to detect unauthorized access and security breaches, thereby ensuring confidentiality, integrity, and controlled data sharing.

A. Research Design

This study follows an applied experimental research design aimed at developing and evaluating a secure cloud storage management system using blockchain technology.

First, requirements are identified by analyzing current chal-lenges in cloud storage security, including data privacy, in-tegrity, and access control. Based on these requirements, a system architecture is designed that combines cloud storage with blockchain, incorporating encryption, hashing, and access control mechanisms.

The solution is implemented in stages: data encryption and storage in the cloud, blockchain-based metadata recording, searchable encryption for retrieval, and HASBE-based ac-cess control. BLAKE2 hashing is used to ensure integrity verification. Key rotation and monitoring modules are also incorporated.

The implemented system is then tested through simulation to evaluate security, performance, and reliability. Metrics such as access control enforcement, integrity validation, and re-trieval efficiency are measured. Finally, results are analyzed to determine how effectively the proposed model enhances secure collaborative cloud storage compared to traditional centralized approaches.

B. Literature Review

- Jain et al. (2017) presented a survey of cryptographic hashing algorithms used for message authentication and digital signatures. The study compared algorithms such as MD5, SHA, and BLAKE with respect to collision re-sistance, efficiency, and suitability for secure data storage applications.
- Alexopoulos et al. (2018) proposed the integration of blockchain with Collaborative Intrusion Detection Sys-tems (CIDS). Their work demonstrated that blockchain improves trust, accountability, and consensus among dis-tributed monitoring nodes.
- Zheng et al. (2017) [1] provided a comprehensive overview of blockchain technology including architec-ture, consensus mechanisms, and major application do-mains. The paper also discussed challenges such as scalability, privacy, and security.
- Park and Park (2017) examined blockchain security in cloud computing environments. They discussed various cloud use cases and highlighted how blockchain can address issues such as data integrity, trust management, and decentralization.
- Sukhodolskiy and Zapechnikov (2018) introduced a blockchain-based access control system for cloud storage. Their model supports secure retrieval of data stored in untrusted cloud environments by recording access infor-mation on the blockchain.
- Darwish et al. (2020) proposed a hybrid blockchain-based algorithm to enhance privacy and security in cloud stor-age. The approach encrypts user data and stores digital signatures on a decentralized ledger to ensure integrity and resistance to tampering.

C. System Architecture Overview

The proposed system architecture integrates cloud storage with blockchain technology to provide secure data manage-ment in a collaborative environment. The architecture pri-marily consists of four entities: data owner, cloud server, blockchain network, and authorized users. The data owner en-crypts files locally and uploads only the encrypted data to the cloud, while corresponding metadata such as file index, hash value, and access information are recorded on the blockchain to ensure immutability and transparency.

Authorized users generate search queries using trapdoor-based searchable encryption to locate required files. Access control is enforced using Hierarchical Attribute-Based Encryp-tion (HASBE), allowing only users with valid attributes and secret keys to decrypt the requested data.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

The blockchain net-work maintains tamper-proof logs of transactions, key updates, and file references, thereby eliminating the need to trust a single cloud provider.

Data integrity is verified using cryptographic hash functions, specifically BLAKE2, which detects any unauthorized modification of stored data. Periodic key rotation and auditing mechanisms are incorporated to further enhance security and resilience against attacks. Overall, the architecture ensures confidentiality, integrity, availability, and fine-grained access control for cloud-stored data in a decentralized manner.

[Fig. 1: Simulation environment setup]

Fig. 1. Simulation environment setup.

[Fig. 2: Network and cloud interaction model]

Fig. 2. Network and cloud interaction model.

[Fig. 3: Blockchain-based storage workflow]

Fig. 3. Blockchain-based storage workflow.

D. Mathematical Formulation

The proposed system uses encryption, hashing, searchable encryption, and key rotation mechanisms to ensure secure data storage and controlled access in the cloud environment.

The plaintext data D is first encrypted using a secret key K_s before outsourcing to the cloud as:

$$C = E(D, K_s) \quad (1)$$

where C represents the ciphertext stored in the cloud. Autho-rized users possessing the correct secret key can recover the original data through:

$$D = E^{-1}(C, K_s) \quad (2)$$

To guarantee the integrity of stored data, a cryptographic hash function $H(\cdot)$ such as BLAKE2 is applied:

$$h = H(D) \quad (3)$$

Integrity verification is successful when the recomputed hash matches the original stored value:

$$H(D_{\text{received}}) = H(D_{\text{original}}) \quad (4)$$

Searchable encryption is supported through trapdoor gener-ation for a query q using key K_t:

$$T = T(q, K_t) \quad (5)$$

To enhance long-term security, keys are periodically updated using a key-evolution function:

$$K_{\text{new}} = F(K_{\text{old}}, t) \quad (6)$$

E. Operational Workflow

The operational workflow of the proposed system consists of four major stages: data encryption, blockchain recording, access control enforcement, and secure retrieval. In the first stage, the data owner encrypts files locally before upload-ing them to the cloud. Only ciphertext is stored in the cloud, whereas metadata and hash values are recorded on the blockchain to ensure immutability.

In the next stage, fine-grained access control is enforced us-ing hierarchical attribute-based encryption. Users are assigned attributes and secret keys according to their roles. Authorized users generate trapdoor search tokens to locate encrypted data without revealing actual keywords.

During the retrieval stage, an authorized user downloads the encrypted file from the cloud and decrypts it using the issued secret or aggregate key. Finally, integrity verification is performed by comparing hash values stored on the blockchain with those computed from the retrieved data. This workflow ensures confidentiality, integrity, transparency, and secure ac-cess without relying on a fully trusted third party.

IV. Results And Discussion

This section presents the results obtained from the im-plementation of the proposed blockchain-based secure cloud storage system and discusses their significance. The evaluation emphasizes security, storage efficiency, access control perfor-mance, and integrity verification.

The system was simulated by uploading encrypted files to the cloud while storing metadata and hash values on the blockchain. Authorized users retrieved files through trapdoor-based searchable encryption and decrypted them using valid secret keys. The results demonstrate that blockchain integra-tion successfully prevents unauthorized modification of stored data and ensures transparency through immutable records.

A. Storage and Access Performance

Table I shows the average time required for three major operations: encryption, blockchain write, and data retrieval. The results indicate that the slight overhead introduced by blockchain logging is acceptable compared with the security benefits offered.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

TABLE I
OPERATION TIME ANALYSIS

Operation	Average Time (ms)
File Encryption	42
Blockchain Metadata Write	58
File Retrieval and Decryption	49

The results show that encryption and decryption operations contribute most of the time consumption, while blockchain transactions add moderate overhead. However, access times remain within acceptable limits for collaborative cloud storage applications.

B. Integrity Verification and Security Evaluation

The BLAKE2 hashing algorithm was used to verify data integrity. Any alteration in a stored data block resulted in a mismatch between computed and stored hash values, success-fully detecting tampering attempts.

Table II summarizes the observed security properties of the proposed system.

TABLE II
SECURITY FEATURE EVALUATION

Security Property	Achieved
Data Confidentiality	Yes
Fine-grained Access Control	Yes
Integrity Verification via Hashing	Yes
Resistance to Unauthorized Modification	Yes
Decentralized Trust Management	Yes

C. Discussion

The results confirm that integrating blockchain with cloud storage enhances:

- confidentiality through data encryption,
- integrity through BLAKE2 hashing,
- transparency through immutable blockchain records,
- secure search via trapdoor-based searchable encryption, and
- fine-grained user authorization using HASBE.

The trade-off is a moderate computational and time over-head arising from cryptographic operations and blockchain transactions. However, these costs are justified as they signifi-cantly improve data protection in collaborative environments. Overall, the proposed system demonstrates improved secu-rity, controlled data sharing, and reliable integrity verification compared with traditional centralized cloud storage mechanisms.

REFERENCES

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus and future trends," in Proc. IEEE Int. Congr. Big Data, 2017, pp. 557–564.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[3] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation Review, vol. 2, pp. 6–19, 2016.

[4] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[5] A. Dorri, S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in Proc. IEEE PerCom Workshops, 2017, pp. 618–623.

[6] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," Peer-to-Peer Netw. Appl., vol. 10, pp. 983–994, 2017.

[7] H. Wang, Y. Song, and X. Wang, "Secure cloud storage based on blockchain and data auditing," IEEE Access, vol. 8, pp. 216995–217006, 2020.

[8] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," Journal of Network and Computer Applications, vol. 79, pp. 88–115, 2017.

[9] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," Information, vol. 8, no. 2, p. 44, 2017.

[10] M. Ali, J. Nelson, R. Shea, and M. Freedman, "Blockstack: A global naming and storage system secured by blockchain," in Proc. USENIX ATC, 2016, pp. 181–194.

[11] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 6, pp. 1615–1625, 2014.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM, 2010, pp. 534–542.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryp-tion for fine-grained access control of encrypted data," in Proc. ACM CCS, 2006, pp. 89–98.

[14] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proc. EUROCRYPT, 2011, pp. 568–588.

[15] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 384–394, 2014.

[16] J. Xu, A. Soltani, M. Jadliwala, and V. Chakravarthy, "Lightweight and robust security-aware multi-factor authentication for smart IoT devices," IEEE Internet Things J., vol. 6, no. 4, pp. 6853–6866, 2019.

[17] P. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE SPW, 2015, pp. 180–184.

[18] S. Singh and N. Singh, "Blockchain: Future of financial and cybersecu-rity," in Proc. 2nd Int. Conf. Contemporary Comput. Informatics, 2016, pp. 463–467.

[19] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in Proc. CRYPTO, 1992, pp. 139–147.

[20] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.

[21] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. PKC, 2011, pp. 53–70.

[22] J. Benet, "IPFS—content addressed, versioned, P2P file system," arXiv:1407.3561, 2014.

[23] A. Azaria, A. Ekblaw, T. Vieira, and A. Pentland, "MedRec: Using blockchain for medical data access and permission management," in Proc. IEEE Open Big Data Conf., 2016, pp. 25–30.

[24] R. K. L. Ko, P. Jagadpramana et al., "TrustCloud: A framework for accountability and trust in cloud computing," in Proc. IEEE Services, 2011, pp. 584–588.

[25] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, 2014.