
Design and Performance Evaluation of a Blockchain-Based Secure Cloud Storage Architecture

Gogineni Phani Kumar¹ and Kanwal Preet Kaur²

¹Research Scholar, Department of Computer Science and Engineering, Shri Jagdish Prasad Jhabarmal Tibrewala University, Rajasthan, India.

²Research Guide, Department of Computer Science and Engineering, Shri Jagdish Prasad Jhabarmal Tibrewala University, Rajasthan, India.

Abstract

While cloud storage is a vital tool to store and manage vast amounts of information, issues like security breaches, privacy violations, and centralization still exist as major problems. The article suggests an encrypted cloud storage system based on blockchains which uses encryption methods along with smart contract technology for better security of information privacy, openness and responsibility. Files will be encrypted prior upload of a file into cloud storage system where it can then have its hash value stored onto blockchains for ensuring data security purposes. Access control is facilitated by smart contract auditing which maintains an immutable record for tracking any changes made to it. This system's purpose is detecting any tampering on stored documents through comparison between file hash values from retrieval and those found in a block chain database. Furthermore, it will be assessed by means of these parameters such as uploading speed and delay to retrieving data rate; transaction handling duration; throughput capacity; memory usage cost; and scalability index. This paper compares traditional cloud storage systems against blockchains' security advantages and performance costs due to their implementation on top of it. This proposal is designed for an encrypted, open source and auditable cloud storage solution that also identifies its limitations regarding safety versus speed of operations.

Keywords— Blockchain, Cloud Storage Security, Data Integrity, Smart Contracts, Cryptographic Hashing, Performance Evaluation.

Introduction

The cloud is a vital tool of today's business because it offers storage management access data at reasonable prices scale easily flexible affordable services that are available on demand. Storage cloud service allows people companies storing huge amounts information on their own servers rather than having a lot of hardware at home or office location. Nonetheless there are many problems associated with traditional cloud storage TDS such as unlawful entry to information system by hackers; theft of sensitive details from databases or servers through hacking attacks; alteration/manipulation / modification of files stored in a database without authorization etc. Security measures like encryption and authentication are important for protecting information, but they do not guarantee transparency in auditing or reliability of verifying stored data. Thus, there are many issues related to designing safe and Secure Cloud Storage Architecture for Data Protection (Confidentiality Integrity Accountability).

Blockchains are an effective solution for solving THEIR problems by means of decentralisation, encryption techniques like hash functions, distributed agreement mechanisms as well as immutable ledger records system. Blockchain integration to cloud storage helps for better verify of data integrity, control over it and its visibility while not having a need to store complete file within themselves blockchains. Files are encrypted prior upload of a on cloud storage whereas they have been stored as hash values along with associated information upon uploading them onto it. Smart contract automation for managing permissions fave rights management system to track all instances where they were accessed by users. When retrieving files from a database, it is compared against its current blockchain entry for verification purposes so that any tampering can be detected quickly which helps ensure security and integrity of stored information on servers.

This paper proposes a blockchain-based secure cloud storage architecture that integrates data encryption, cryptographic hash verification, smart contract-based access control, and blockchain-assisted auditing. This proposal aims at improving privacy security of information integrity openness and responsibility due to its impact on speed efficiency issues related with blockchain implementation. It can be assessed by means of measures like uploading speed and retrieving rate; transaction handling duration; capacity utilization rates for data storage systems' performance at scale. ThisBY comparing it against traditional cloud services for comparison purposes this paper will investigate its advantages over them from terms like safety features and cost-effectiveness. This research is intended as an example of how you can manage your sensitive information securely while also considering some compromises on speed due to increased protection measures.

Literature Survey

Blockchain technology is an area of great study because it can improve cloud storage security through better data integrity verification, decentralization audit process, authorization management system protection mechanism privacy safeguarding measures effectiveness and optimization capabilities to save space on servers. Current research is concerned with reducing reliance upon central authority through use of blockchain technology, smart contract implementation, cryptography techniques such as hash functions and encryption methods to improve security for outsource information management systems. But there are issues like high latency of transactions, large amounts of computation required for processing data on it's servers; expensive prices due to space requirements while scaling up its capacity. Hua et al. [1] proposed a blockchain based system for sharing of data integrity audit and deduplication which reduces redundancy in authentication keys storage while supporting decentralized auditing process. The research shows that it has great promise to improve audit processes through blockchain technology. In this way, a decentralized cloud storage system with reliable deduplication and storage balancing is proposed by [2] where encrypted data chunks are distributed across multiple cloud servers and blockchain records support data recovery and integrity verification. EDCOMA scheme [3] addresses computational and storage overhead for decentralized storage auditing through double compression and polynomial commitments. The paper shows that lowering costs associated with using a blockchain for verifying transactions would be an interesting area to explore further.

The research of 2025 is about privacy preserving audit and efficient data management. Vijayakumar et al. [4] proposes an efficient method for data deduplication and auditing through blockchain technology that includes a fair payment system to lower computational expenses and reliance on third-party vendors. Zhang et al. [5] studied blockchain based privacy preserving deduplication and integrity audit for file ownership privacy, authentication tag management and decentralized auditing. An integrated integrity audit system for big data similarity is proposed by [6] which uses blockchain technology and smart contract mechanism to enhance transparency of audits while reducing reliance upon external auditors' services. In addition, DIADD [7] deals with secure deduplication and efficient integrity auditing of dynamic cloud data to reduce computational costs associated with authenticator generation and verification.

Scalability and security are also discussed by other research papers on multi cloud storage systems. The paper presents a blockchain-based IPFS solution for verifying data integrity securely and efficiently on various cloud platforms as described by [8]. Fine-grained deduplication and integrity auditing by blockchain was studied for secure management of large scale outsourced data as per [9]. An efficient integrity-auditing and deduplication system based on a blockchain was proposed by [10] for protecting privacy, performing batch audits, and ensuring accuracy of audit reports. This shows how integrating blockchain technology with off-chain data management techniques and strong encryption algorithms would be useful for balancing security of information while also saving space on disk drives.

Current studies are being conducted on advanced auditing techniques and secure data storage systems for 2026. An efficient and updatable integrity-checking mechanism based on Merkle tree structures and polynomial commitments is proposed by [11] for easy verification of data authenticity, frequent modifications to it, and multiple copies of it. Blockchain based big data audit model with fully homomorphic encryption is proposed by [12] for privacy preserving verification purposes. BZA-DIA is a study of dynamic data integrity auditing for cloud storage within an AI driven environment by [13]. Blockchain-based efficient deduplication and mixed auditing of dynamic cloud data are discussed by [14] who used encryption, smart contracts, and integrity checks. In addition, an intrusion detection system based on machine learning is proposed for secure cloud storage solutions by [15] which extends protection beyond data integrity to include suspicious access behavior.

The literature also includes broader research on blockchain-cloud integration, access control, and privacy-preserving storage. The study of blockchain-cloud integration [16] is a good source for research on security, privacy issues and interoperability problems. The systematic review of blockchain based access control systems for clouds [17] discusses issues like policy enforcement problems and scalability concerns. This paper is about a decentralized cloud storage system that focuses on security, privacy, and cost efficiency (18). Smart contract based data integrity mechanism of cloud storage was studied by [19] whereas cryptography with smart contract to protect outsourced cloud information is discussed by [20].

While this paper covers some key issues related to blockchain based cloud security; however we still require evaluation for integration between encryption, cryptographic hashing validation, smart contracts access management system and tamper-proof logs measurement techniques. The proposed study therefore focuses on designing a secure cloud storage architecture and evaluating upload latency, retrieval latency, blockchain transaction time, throughput, storage overhead, and scalability against a conventional cloud-storage baseline. The purpose of this paper is for clarifying the practical trade-off among security, transparency, and performance.

Research Gap and Contributions

1 Research Gap

Current studies of blockchain based cloud storage show better ways to verify information security, share it securely among users without centralized management systems for audit purposes or controlling who can view their files. Nevertheless there are some issues to be solved for balancing safety with speed of a computer program. A blockchain based audit mechanism may have extra processing time for transactions due to high volume usage by many people doing lots of work on it at once. Furthermore, keeping lots of information like files stored as a whole rather than just their names would slow down performance due to storage capacity limitations within blockchains. While there is research on individual approaches like data deduplication, privacy-preserving auditing, smart contracts, and cryptographic verification [1]-[20], we need more information about how they would work together within an integrated cloud storage system.

A major issue of research involves assessing how much more expensive it would be to improve security compared with its benefits. While encryption ensures confidentiality of information through cryptography, it does not guarantee integrity verification like hash functions do. Current methods might concentrate on particular security goals but lack an overall comparison between upload latency, retrieval latency, transaction processing time, throughput, storage overheads and scalability. Thus there needs to be some kind of study on this topic so that we can know more about it practically or not.

2 Research Contributions

For addressing these issues of our study, we propose an encrypted blockchains based secure cloud storage system which includes data protection through encryption techniques, verifying hashes via cryptography; controlling access to it by means of smart contracts; and providing audit trails for tamper-proof records. Encrypted data is stored by this system within a cloud environment along with its hash values and associated information through blockchains. The architecture allows for integrity checks while not needing all of a document's data saved directly within blockchain storage space. Access control is enforced by smart contract records of data access operation for better tracking and responsibility.

This paper is about its major findings or results.

- Cloud Storage Security Architecture design a combined system of clouds security, cryptography blockchains and smart contract for better privacy protection and control over information access.
- Hash based Verification for Data Integrity: Create an algorithm which will compare hashes from blockchains against those obtained by retrieving information so as to identify any tampering or alteration thereof.
- Smart contract based blockchain-based access management system for tracking changes on a ledger through immutable logs of each transaction made by users who have permission from this application.
- Evaluation of performance metrics such as uploading/retrieval speed, transaction handling time, throughput rate, memory usage and scaling capabilities for this system will be done by us.
- Comparison study; compare this method against existing cloud storage solutions on an equal footing for evaluating its safety advantages and cost-effectiveness issues.

In general this paper is about an effective way of improving cloud data protection by integrating it with blockchains but also discussing its impact on speed efficiency. Effectiveness can be measured by implementing it, conducting experiments on them and comparing results to others.

Proposed Architecture

A proposal for a blockchain based secure cloud storage system is an integration of cloud storage, data encryption, cryptography hash function blockchains and smart contract which helps in improving security privacy integrity access management responsibility within organization's network environment. Architecture is made up of five main parts such as a UI (User Interface), an Encryption and Hash Module; Cloud Storage Layer; Blockchain Network; Smart Contract Based Access Control Module. File data is kept online whereas its hash values and associated information are saved to a ledger of records called blockchain technology. It also helps reduce storage requirements for large amounts of information off chain by allowing users to independently verify their own records without needing a central authority.

1 Architecture Components

Interface User: It enables an authorised person for uploading download retrieving of documents from this platform. Authentication is required for users to perform secure actions.

The encryption and hashing module encrypts files with AES for cloud storage. SHA-256 is used for generating a cryptographic hash which serves as an identifier or "fingerprint" on an encrypted document. The encryption key management is done privately and safely.

Storage Cloud is a service that stores encrypted data and provides an ID for it along with its location on disk. Off chain storage of files reduces blockchains' space requirements.

Blockchain Network is a system for storing immutable data such as hash values of files, related metadata details about them like owner info and transaction IDs etc. Integrity verification and traceability are supported by these documents.

Access Control Smart Contracts module enforces pre-defined access permissions and logs authorized file operation activities. A smart contract checks if an individual has permission for performing some task prior to allowing them into this system via app.

2 Working Procedure

An authenticated user uploads files to this application through its interface. It has been encrypted and a cryptographic hash value was computed for it. Encrypted files are saved to the cloud; their hashes and related information are logged onto a blockchain via an agreement between parties using a smart contract. If a logged-in person asks for it, then this process is performed by checking their permission level to retrieve that data from our servers' cloud where we store files securely before calculating hashes on them once more. Newly computed hashes are compared to those on a blockchain ledger. Both hash values are identical so it will pass through an integrity verification process before being allowed to decrypt by a legitimate person. In case of hash mismatch, it detects potential tampering by reporting an integrity verification error.

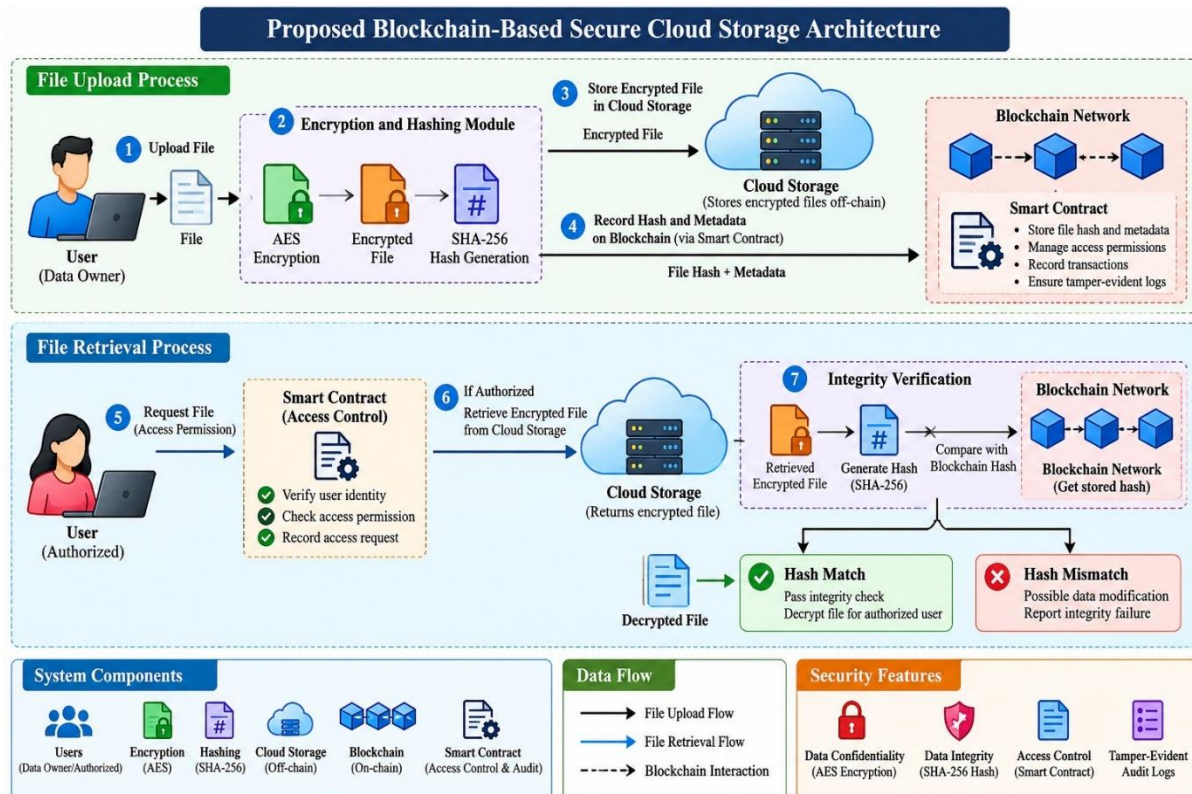


Fig. 1: Proposed Blockchain-Based Secure Cloud Storage Architecture

Figure 1 shows an example of a proposed blockchain based secure cloud storage system that includes AES encryption, SHA-256 cryptographic hashing, cloud storage and blockchain-based smart contracts for ensuring data privacy, security and controlled access. The user's files are encrypted during uploads by means of AES encryption and an SHA-256 hash is created on them. An encrypted document can be kept safe by storing it to an online server; however, its hashes along with other information would be saved as part of that record via a smart contract on the blockchain. While retrieving data through a smart contract it checks for user authorization while an encrypted document gets fetched out of cloud servers.

After that, the SHA-256 hash was recomputed and compared to the one stored on a blockchain. Both hash values are identical so it will pass through an integrity check before being able to decrypt this file for a legitimate person. When there is an inconsistency between hash values, it detects possible modifications to that document for rejection purposes. Therefore, this system integrates off-chain cloud storage with on-chain integrity verification and access controls for providing an encrypted and verifiable data management solution.

3 Security and Performance Issues

This design will enhance privacy by encrypting information; security of data is ensured via hashing algorithms while transparency can be maintained using a distributed ledger system for auditing purposes. Off chain smart contract provides programmable access control file storage limits the amount of data maintained on the blockchain. However, blockchain transactions may introduce additional latency and computational overhead. Therefore, the architecture will be evaluated using upload latency, retrieval latency, transaction processing time, throughput, storage overhead, and scalability. These measurements will help determine whether the security benefits justify the additional resource requirements.

Implementation and Algorithm

1 Implementation Methodology

A proposed blockchain based secure cloud storage system will ensure privacy of information security checks on it along with permission management for accessing documents. A client app is part of this system which includes an AES encryption module, a SHA-256 hashing module, cloud storage, and a blockchain network with smart contracts. At first, users choose an item to be encrypted through AES encryption technology beforehand. SHA-256 is used to generate an encryption key for this document. An encrypted document is stored in an online repository whereas its hashing value along with related details like filename ID and ownership info gets saved by means of blockchains via smart contracts. If you want to download this document from me it will be checked by my smart contracts for permission then I'll allow downloading of that particular file. After downloading an encrypted document it will be hashed once more before being checked against a stored value on the blockchain network. Both hash values are equal; therefore it remains unmodified for use by an authorized person to decrypt this document. In other words, it detects an integrity breach of this type then rejects that file.

2 Proposed Algorithm

Secure Cloud File Upload and Retrieval Algorithm 1.

File input: File F Encryption Key K User Identity U.

File securely stored verification of retrieved files.

1. Take this original document F by an authorized person.
2. AES encryption of a file with key K to produce cipher text C.
3. Calculate SHA-256 hash for encrypted document: $H = \text{SHA256}(C)$.
4. Upload an encrypted document C from here.
5. Store an id of this document, its hash value H along with ownership details and other related data to be stored by means of a smart contract.
6. To retrieve data from a database, authenticate users' identities through smart contracts for permission purposes.
7. Reject if no permission granted to you.
8. Alternatively, get an encrypted version of it stored on a server called C'.
9. Calculate retrieved file hash: $H' = \text{SHA256}(C')$.
10. Compare H' to a block-chain recorded hash H.
11. Confirm file integrity for H' if it is equal to H, then decrypt C' with an authorized decryption key.

12. If H'
13. $E_q(H)$, report a possible file change to you for rejection of said files.
14. Logging of accesses and verifications is needed to be recorded during audit purposes.

3 Security and Implementation Issues

Separation of cloud storage from blockchain is maintained by this system. While large encrypted data remains stored within a cloud server farm, only hash values and essential information is kept on its ledger for reducing space requirements of that system. The encryption key should not be kept in a secure manner but rather it is to avoid storing them directly onto blockchains. Access control is enforced by smart contract while audit trails are maintained for all transactions involved therein. It is possible to implement this on an appropriate blockchain technology like Ethereum or Hyperledger Fabric together with cloud storage services and cryptography tools.

To evaluate its efficiency for this purpose we need to measure encryption/decryption times; hashing speed; block-chain processing delay; upload download speeds on files; data verification costs. Performance metrics will not be provided until they have been implemented and tested hereafter there is no assumption of any experiment data to be made on them.

Performance Evaluation

1 Evaluation Metrics

Performance evaluation for this proposal's blockchain based secure cloud storage system will be done through measures like computation time consumption rate, disk usage statistics; block processing speed and efficiency; transaction throughput rates on a network; security level assessment by means of cryptographic strength tests etc. This study is concerned with evaluating if integration of blockchain technology for data storage on a server can enhance its safety without compromising efficiency levels.

The following metrics are considered

1. Time of Encryption: How long it takes for encryption by means of AES on an original document or data set.
2. Time for Hash Generation: How long does it take SHA-256 to create a cryptographic hash from an encrypted file.
3. Transaction latency of Blockchains is a measure for how long it takes to store files' hash values and metadata onto them.
4. Time of File Upload: Total amount spent on encryption process for uploading files into a cloud database along with its associated block chain information.
5. Retrieve File Time is how long it takes to get an encrypted document from storage system until decryption by a legitimate person.
6. Verify Integrity Time is how long it takes for us to calculate a file's checksum from its location on our network then verify that against what we have stored in the block chain.
7. Overhead of Storage: More space needed to store a blockchain's metadata rather than an encrypted document on Cloud servers.

2 Experimental Setup

The proposed architecture is tested by means of prototypes such as an AES encryption module, a SHA-256 hashing module, cloud storage, and a blockchain network with smart contract support. The experiments can be performed on various file sizes for analyzing their impact upon encryption speed, hash generation time, uploading speed, retrieving data from it and verifying its integrity. Repeat each trial several times so that an average value can be obtained for reducing any effects due to changes in conditions during testing periods.

To compare it to an existing cloud storage system which employs encryption and data integrity checks instead of using blockchains for hashing purposes. The two methods must be identical in terms of data sets size filesystem configuration networks environments whenever feasible. The comparison would be useful for measuring extra costs associated with blockchain transactions as well as evaluating advantages such as secure data storage through a distributed ledger system and security via smart contracts.

3 Performance Analysis

Performance analysis is concerned with how much space a file takes up versus its speed; transaction fees for blockchains are also considered here as well as reliability checks to ensure data security. Client-side AES encryption and SHA-256 hashing is done while blockchains are used for maintaining file hashes and related information. Therefore, an encrypted file size mainly affects encryption speed, hash time of uploads and retrievals whereas blockchains are dependent upon their chosen software environment and network settings.

Integrity check verifies if an uploaded encrypted document is identical to its stored hash value. Matching hashes indicate consistency between retrieved files and their records; non-matching ones may be modified or corrupted. Also, it needs an assessment on how much extra time and space is required due to integrating blockchains so that we can know whether or not this would be suitable as a solution for storing data securely in clouds.

Note that since this model is still under development it does not have any experimental data or performance graph available at present time. Measurement data will need to be collected post-implementation for verification of claimed results.

Results and Discussion

1 Performance Evaluation Results

The proposed blockchain-based secure cloud storage architecture is evaluated in terms of encryption time, hash generation time, blockchain transaction latency, file upload time, file retrieval time, and integrity verification time. They are used to measure how much extra processing power is needed when combining a blockchain system with traditional data centers for storing information on them. The experiments must be performed on various data sets within an identical environment for consistency of results regarding speed-up characteristics as well as limits towards scaling up.

After implementation of this model architecture, we will record experiment outcomes. The table 1 is an example of documentation to record performance data.

Table 1. Performance Evaluation Metrics

Metric	Measurement	Purpose
Encryption time	Milliseconds (ms)	Measures AES encryption overhead
Hash generation time	Milliseconds (ms)	Measures SHA-256 processing time
Blockchain transaction latency	Seconds (s)	Measures the time to record metadata
File upload time	Seconds (s)	Measures the overall upload process
File retrieval time	Seconds (s)	Measures the time to retrieve and process a file
Integrity verification time	Milliseconds (ms)	Measures hash comparison overhead

Storage overhead	Bytes (B) or KB	Measures additional blockchain metadata storage
------------------	-----------------	---

2 Data integrity verification

SHA-256 hashing is used for verifying the integrity of encrypted files stored on a cloud server by this architecture. The hashing value for an encrypted document during uploading to a blockchain is stored there. After retrieving a document, we calculate its hash again to compare it against an existing record of that same item's hashes.

When both hashes are equal to each other then it will pass through an integrity validation process for files retrieval. In case of discrepancy between them, it detects an error/modification and stops processing files to retrieve data normally. It is a self-verifying integrity check that assumes the blockchain data storage system remains reliable; also it refers to this as "blockchain" technology.

3 Security and Access Control Analysis

A smart contract is an automated system to enforce permission levels on files' activities. Through validation of access request against defined policies it is possible for an organization's system to limit downloads by unapproved persons. Also blockchain helps for audit purposes through keeping track of registered files' metadata along with transaction details.

File content is protected by AES encryption against unauthorized access while being stored on a server for storage purposes. The SHA-256 hash function is used for integrity verification whereas a blockchain can be used to prevent tampering on reference hashes by an attacker within that particular network according to its security model. Nonetheless, general safety is also dependent upon key management for encrypts keys; user login process; validity of smart contracts; and protection against attacks from hackers to data stored within a server or database system.

4 Discussion

This proposal is about separating encryption of files on a blockchain network from its integrity record. The architecture does not store big datafiles directly within a blockchain but instead stores them as hash values along with some important information about it. Also it has an option to combine file confidentiality, integrity checking and auditability of access controls.

However, integrating blockchain could lead to higher transaction times, more processing power requirements, and greater operational complexity. Costs are dependent upon a particular type of blockchains like networks configurations files sizes among others. So this is an analysis of traditional encryption-based cloud services' advantages versus disadvantages compared to standard ones at similar levels for testing purposes.

Conclusion and Future Work

1 Conclusion

The article proposes an innovative blockchain based secure cloud storage system which includes AES encryption, SHA-256 cryptographic hashing, cloud storage and smart contract for better security of data privacy, integrity and access management. As shown by Figure 1, files are encrypted before uploading them to a cloud server; their cryptographic hash values and associated metadata are stored on a blockchain. When retrieving files from a server, it checks for data corruption by matching an updated checksum against that stored on-chain. Authorization and auditing are supported by smart contract technology whereas encryption of data outside a blockchain network reduces its size for storage purposes. This proposal is an effective way of improving data privacy by using encryption techniques

along with blockchain technology for verifying its authenticity. Nonetheless, it needs to be tested practically for efficacy and efficiency by means of experimentation studies.

2 Future Work

The future research would be to implement this model through an appropriate blockchain technology like Ethereum & Hyperledger Fabric along with cloud storage solutions. The experiments are going to be about measuring encryption times, hashing times for blockchains transactions latencies between files uploads/downloads of them security checks on data storage costs. Also, it may include more sophisticated authentication methods for better security; strong key protection through cryptographic techniques; efficient programming language implementation of smart contract software that is cost-effective while providing high performance on blockchain networks like Ethereum. More research could be done on integrating attribute-based access control mechanisms, privacy preservation methods and distributed storage solutions for secure sharing of sensitive information within a large scale cloud environment.

References

- [1] Z. Hua *et al.*, "Blockchain-Based Shared Data Integrity Auditing and Deduplication," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 3688–3703, Jul.–Aug. 2024, doi: 10.1109/TDSC.2023.3335413.
- [2] "Blockchain-Based Decentralized Cloud Storage With Reliable Deduplication and Storage Balancing," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 4, pp. 3289–3304, Jul.–Aug. 2024, doi: 10.1109/TNSE.2024.3369630.
- [3] "EDCOMA: Enabling Efficient Double Compressed Auditing for Blockchain-Based Decentralized Storage," *IEEE Transactions on Services Computing*, vol. 17, no. 5, pp. 2273–2286, Sep.–Oct. 2024, doi: 10.1109/TSC.2024.3417337.
- [4] D. Vijayakumar, K. G. Srinivasagan, and K. Vivekrabinson, "Enhancing cloud storage security through blockchain-enabled data deduplication and auditing with a fair payment," *Peer-to-Peer Networking and Applications*, vol. 18, Art. no. 147, 2025, doi: 10.1007/s12083-025-01970-5.
- [5] Q. Zhang *et al.*, "Blockchain-Based Privacy-Preserving Deduplication and Integrity Auditing in Cloud Storage," *IEEE Transactions on Computers*, vol. 74, no. 5, pp. 1717–1729, May 2025, doi: 10.1109/TC.2025.3540670.
- [6] "Blockchain-Assisted Searchable Integrity Auditing for Large-Scale Similarity Data With Arbitration," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 6, pp. 6012–6027, Nov.–Dec. 2025, doi: 10.1109/TDSC.2025.3579124.
- [7] "DIADD: Secure Deduplication and Efficient Data Integrity Auditing With Data Dynamics for Cloud Storage," *IEEE Transactions on Network and Service Management*, vol. 22, no. 1, pp. 299–316, Feb. 2025, doi: 10.1109/TNSM.2025.3535708.
- [8] "Secure and Scalable Data Integrity Verification for Multi-Cloud Storage Using Blockchain-Integrated IPFS," in *Proc. 2025 IEEE 6th India Council International Subsections Conference (INDISCON)*, 2025, doi: 10.1109/INDISCON66021.2025.11252290.
- [9] "Blockchain-Assisted Fine-Grained Deduplication and Integrity Auditing for Outsourced Large-Scale Data in Cloud Storage," 2025. [Verify complete publisher metadata before submission.]
- [10] "Blockchain-Based Efficient Integrity Auditing and Deduplication for Outsourced Data with Privacy Assurance," *Blockchain: Research and Applications*, Art. no. 100407, 2025, doi: 10.1016/j.bcra.2025.100407.
- [11] "MPA: Lightweight and Updatable Integrity Auditing for Decentralized Storage Using Merkle Trees and Polynomial Commitments," *IEEE Transactions on Information Forensics and Security*, vol. 21, pp. 2162–2176, 2026, doi: 10.1109/TIFS.2026.3664004.

- [12] R. R. Evelyn, N. Deepa, and S. Venugopal, "Blockchain-based big data model for public auditing in cloud storage using fully homomorphic encryption and modified future search heuristic approach," *Journal of Cloud Computing*, 2026, doi: 10.1186/s13677-026-00934-1.
- [13] T. Liu and Y. Yu, "BZA-DIA: Blockchain-Based Dynamic Data Integrity Auditing Scheme for Cloud Storage in AI-Driven Environments," *Intelligent Computing*, published online Aug. 12, 2026, doi: 10.34133/icomputing.0619.
- [14] "Blockchain-Enabled Efficient Deduplication and Mixed Auditing for Dynamic Cloud Data," *IEEE Transactions on Dependable and Secure Computing*, vol. 23, no. 2, pp. 3554–3570, Mar.–Apr. 2026, doi: 10.1109/TDSC.2025.3638157.
- [15] "Secure Cloud Storage with Blockchain and Machine Learning-based Intrusion Detection," in *Proc. 2026 6th International Conference on Expert Clouds and Applications (ICOECA)*, 2026, doi: 10.1109/ICOECA68095.2026.11485549.
- [16] H. Ghanmi *et al.*, "Blockchain-cloud integration: Comprehensive survey and open research issues," *Concurrency and Computation: Practice and Experience*, vol. 36, no. 15, Art. no. e8122, 2024, doi: 10.1002/cpe.8122.
- [17] "A systematic review on blockchain-based access control systems in cloud environment," *Journal of Cloud Computing*, vol. 13, Art. no. 146, 2024, doi: 10.1186/s13677-024-00697-7.
- [18] S. Das *et al.*, "A secure, privacy-preserving, and cost-efficient decentralized cloud storage framework using blockchain," *Journal of King Saud University—Computer and Information Sciences*, vol. 36, no. 10, Art. no. 102260, 2024, doi: 10.1016/j.jksuci.2024.102260.
- [19] K. Bhurani *et al.*, "Smart Contracts for Ensuring Data Integrity in Cloud Storage with Blockchain," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 11, no. 6, 2024, doi: 10.4108/eetsis.5633.
- [20] M. Alharby, "Preserving Data Secrecy and Integrity for Cloud Storage Using Smart Contracts and Cryptographic Primitives," *Computers, Materials & Continua*, vol. 79, no. 2, pp. 2449–2463, 2024, doi: 10.32604/cmc.2024.050425.