# Blockchain-Assisted Data Integrity Auditing for Cloud Environments

**K. Pavani[1], Mr.jakkula venkat rayudu[2],**
**#1 Assistant Professor & Head of Department of MCA, SRK Institute of Technology, Vijayawada.**

**#2 Student in the Department of MCA, SRK Institute of Technology, Vijayawada.**

**Abstract:** Data integrity and secure data storage have become major concerns in modern cloud computing environments due to the rapid growth of digital information and online data sharing. Traditional centralized storage systems are vulnerable to unauthorized access, data tampering, insider attacks, and single points of failure, making it difficult to guarantee the authenticity and reliability of stored information. To address these security challenges, this project proposes a Data Integrity Audit Scheme Based on Blockchain Expansion Technology that utilizes blockchain technology to provide secure, transparent, and tamper-resistant data auditing mechanisms.

The proposed system replaces conventional third-party auditing methods with a decentralized blockchain-based verification process. In this system, uploaded data is converted into unique hash values using the SHA cryptographic hashing algorithm, and these hash values are securely stored on the blockchain network. Any unauthorized modification in the data automatically changes the hash value, enabling immediate detection of tampering attempts. Due to the immutable and distributed nature of blockchain, data integrity can be verified without relying on centralized authorities or external auditors.

The system is developed using technologies such as Node.js, Express.js, Ethereum Blockchain, JavaScript, HTML, CSS, and Bootstrap. The proposed framework improves security, transparency, reliability, and trust among users while reducing operational overhead and privacy risks associated with traditional auditing systems. Additionally, the decentralized architecture eliminates single points of failure and ensures continuous availability of data verification services.

## 1. INTRODUCTION

When it comes to handling massive volumes of digital data, cloud computing has emerged as a crucial tool. The convenience, adaptability, scalability, and low maintenance cost of cloud storage make it a popular choice among both consumers and businesses. Having said that, there are legitimate security concerns about keeping sensitive information including medical records, financial records, legal papers, and criminal files on servers in the cloud. Keeping data accurate, original, and unaltered throughout its lifetime is one of the biggest challenges in cloud systems.

Users of older, more centralized cloud storage systems had to put their faith in cloud service providers and independent auditors to keep their data safe and secure. Unauthorized changes, cyberattacks, insider threats, and single points of failure are all possibilities for these systems. Security and privacy issues arise when users are unable to readily tell if their data has been altered.

Blockchain technology offers a decentralized and immutable answer to these problems by facilitating secure data audits. The distributed ledger technology known as blockchain makes data accessible and unchangeable by storing it in linked blocks protected by cryptographic hash algorithms. It is easy to identify efforts at manipulation because the hash value changes whenever data is modified.

The goal of this project, "Data Integrity Audit Scheme Based on Blockchain Expansion Technology," is to create a safe system that can check if data is intact by utilizing blockchain technology and SHA hashing algorithms. By storing data hash values on the blockchain, the suggested approach

allows for decentralized verification, eliminating the need for third-party auditors. In addition to lowering operational overhead, the system promotes security, transparency, dependability, and trust. Frameworks like Node.js.

## 2. LITERATURE SURVEY

### 2.1 Data Integrity Verification in the Cloud Using Blockchain Technology

One of the most popular ways to store and organize data digitally is through cloud computing. The security of data and the prevention of unwanted changes are still big concerns in cloud settings. An rise in operating costs and security hazards are associated with traditional cloud storage solutions' reliance on centralized servers and third-party auditors for integrity verification.

As a distributed ledger platform for safe data auditing, researchers have introduced blockchain. Because blockchain records transactions in immutable blocks linked by cryptographic hash algorithms, data tampering is very difficult, if not impossible. Multiple studies have shown that auditing techniques based on the blockchain increase confidence, reliability, and transparency while decreasing reliance on centralized authorities. Additionally, blockchain's decentralized design improves security by removing potential weak spots and cyberattack vectors.

### 2.2 Ensuring Data Integrity through the Use of the Public Key Hashing Algorithm

The security and authenticity of data stored in digital systems rely heavily on cryptographic hashing methods. Every data file gets its own distinct hash value of a specified length generated by the Secure Hash Algorithm (SHA). To make it easier to identify manipulation, even a slight change to the original data results in a totally different hash value. In order to develop auditing systems that are both safe and resistant to tampering, researchers suggested integrating blockchain networks with SHA algorithms. The blockchain stores the produced hash values in an immutable format that cannot be changed without agreement from all nodes in the network. Cloud storage applications benefit from rapid validation, robust security, and efficient performance when using SHA-based integrity verification procedures, according to experimental investigations.

### 2.3 Trustless Blockchain-Based Decentralized Cloud Storage

The use of decentralized blockchain frameworks to strengthen the security of cloud storage was the attention of numerous researchers. Centralized cloud systems as they currently stand are susceptible to threats such as data breaches, server outages, insider assaults, and unauthorized access. These restrictions prompted the development of decentralized storage structures based on the blockchain. These systems guarantee openness and fault tolerance by distributing records over numerous network nodes. The automation of data access control and integrity verification is made possible by smart contracts and consensus algorithms. When compared to more conventional cloud designs, research shows that decentralized blockchain systems vastly improve data trustworthiness, visibility, and immutability.

.

## 3. METHODOLOGY

**i) Proposed Work:**

The proposed system introduces a secure and decentralized Data Integrity Audit Scheme Based on Blockchain Expansion Technology to overcome the limitations of traditional cloud auditing systems. The system uses blockchain technology and SHA cryptographic hashing algorithms to provide secure, transparent, and tamper-resistant integrity verification for cloud-stored data.

In the proposed framework, whenever a user uploads data, the system generates a unique hash value using the SHA hashing algorithm. This hash value acts as a digital fingerprint for the uploaded file. The generated hash value is then stored securely on the blockchain network instead of depending on centralized servers or external auditors. Since blockchain records are immutable and distributed across multiple nodes, unauthorized modifications become extremely difficult.

During integrity verification, the system recalculates the current hash value of the stored data and compares it with the original hash stored on the blockchain. If both hash values match, the data is considered authentic and unmodified. If the hash values differ, the system immediately detects tampering attempts and alerts the user.

Blockchain technology provides decentralization, transparency, fault tolerance, and immutability. Since no single authority controls the network, the proposed system eliminates dependency on third-party auditors and removes single points of failure. All verification records are permanently stored on the blockchain, ensuring secure and transparent auditing.

The system is implemented using technologies such as Node.js, Express.js, Ethereum Blockchain, JavaScript, HTML, CSS, and Bootstrap. The decentralized architecture improves reliability, reduces operational cost, enhances security, and supports efficient real-time integrity verification for modern cloud environments.

The proposed framework can be applied in several security-sensitive domains such as banking, healthcare, legal systems, educational institutions, enterprise cloud storage, and government record management where protecting data integrity is highly important.

**ii) System Architecture:**

System Architecture represents the overall structure and organization of the proposed system. It shows how different components interact with each other to perform secure data integrity auditing. The proposed architecture is designed using blockchain technology, cryptographic hashing algorithms, cloud storage concepts, and decentralized verification mechanisms.

In the proposed system, users interact with the web application through a user-friendly interface developed using HTML, CSS, Bootstrap, and JavaScript. The user uploads data files to the system, and the backend server developed using Node.js and Express.js processes the uploaded information. The SHA hashing algorithm generates a unique cryptographic hash value for every uploaded file.

The generated hash value is stored on the Ethereum blockchain network instead of storing sensitive information directly on centralized servers. Blockchain nodes maintain immutable records of all transactions and integrity verification details. Whenever users perform integrity verification, the system recalculates the hash value of the current file and compares it with the original blockchain hash value.

If both hash values match, the data is considered authentic and unchanged. If the values differ, the system immediately identifies tampering attempts and alerts the user. Since blockchain records are decentralized and immutable, unauthorized modification becomes extremely difficult. The architecture also eliminates dependency on third-party auditors and improves transparency, security, and reliability.

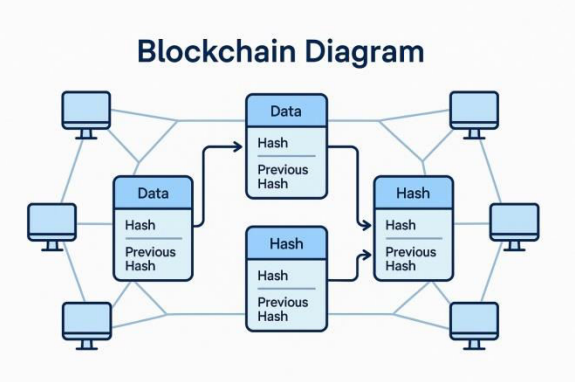



Fig.1. Proposed Architecture

**iii) MODULES:**

**1. User Registration Module**

The User Registration Module allows new users to create accounts in the system by providing personal details such as username, email address, and password. This module validates registration information and securely stores user credentials in the database. The module ensures that duplicate accounts are not created and only authorized users can access the application.

**Functions:**

- User account creation
- Validation of user details

• Password encryption
• Secure storage of credentials

**Advantages:**

• Prevents unauthorized access
• Maintains user identity management
• Improves system security

**2. User Authentication Module**

The User Authentication Module verifies user credentials during login and controls access to the application. This module checks usernames and passwords before granting access to blockchain auditing services. Session management mechanisms are also implemented to maintain secure user communication.

**Functions:**

• User login validation
• Session management
• Access control
• User logout handling

**Advantages:**

• Secure authentication process
• Prevents unauthorized usage
• Protects confidential information

**3. File Upload Module**

The File Upload Module allows users to upload files securely into the blockchain auditing system. Uploaded files are temporarily stored and processed for SHA hash generation and integrity verification. The module validates file formats and prevents unsupported or malicious file uploads.

**Functions:**

• File selection and upload
• File validation
• Temporary file storage
• File management operations

**Advantages:**

• Secure file handling
• Efficient data processing
• Easy user interaction

**4. SHA Hash Generation Module**

The SHA Hash Generation Module is one of the most important components of the system. It generates unique cryptographic hash values for uploaded files using the SHA algorithm. The generated hash value acts as a digital fingerprint of the file and is used for future integrity verification.

**Working Process:**

1. User uploads a file.
2. File data is read by the server.
3. SHA algorithm processes the data.
4. A unique hash value is generated.
5. The hash value is forwarded to the blockchain module.

**Advantages:**

• Unique file identification
• Fast processing speed
• High security
• Tamper detection support

**5. Blockchain Storage Module**

The Blockchain Storage Module stores generated SHA hash values securely on the Ethereum blockchain network. Blockchain transactions are created for each uploaded file, ensuring decentralized and immutable storage of integrity records.

**Functions:**

• Blockchain transaction creation
• Hash value storage
• Transaction verification
• Distributed ledger maintenance

**Advantages:**

• Decentralized auditing
• Immutable records
• Transparent verification
• Eliminates third-party auditors

**6. Integrity Verification Module**

The Integrity Verification Module verifies whether uploaded data has been modified or tampered with. During verification, the system generates a new SHA hash value for the current file and compares it with the original blockchain hash.

**Working Process:**

1. User requests integrity verification.
2. Current file hash is generated.
3. Original blockchain hash is retrieved.
4. Both hash values are compared.
5. Verification result is displayed.

**Advantages:**

• Real-time tampering detection
• Accurate verification results
• Improved data reliability

**7. Alert and Notification Module**

This module generates notifications whenever unauthorized modifications or tampering attempts are detected during integrity verification. Alerts help users identify security threats immediately.

**Functions:**

• Tampering alerts
• Verification result display
• Security notifications
• Error handling

**Advantages:**

• Immediate attack detection
• Improved user awareness
• Real-time monitoring support

**8. Blockchain Network Module**

The Blockchain Network Module manages communication between blockchain nodes and maintains decentralized records securely. Blockchain nodes validate transactions and ensure consistency across the distributed ledger.

**Functions:**

• Node communication
• Transaction validation
• Consensus management
• Blockchain synchronization

**Advantages:**

• High fault tolerance
• Decentralized verification
• Improved transparency
• Permanent record storage

**.iv) ALGORITHMS:**

Algorithms are essential for secure operation and accurate functionality of the proposed blockchain auditing system. The project mainly uses SHA cryptographic hashing algorithms and blockchain verification mechanisms.

**SHA (Secure Hash Algorithm)**

SHA is a cryptographic algorithm used to generate fixed-length unique hash values for uploaded data. Even a small modification in the original file results in a completely different hash value, making tampering detection easier.

**Steps of SHA Algorithm:**

1. Input file is selected.
2. File data is processed into blocks.
3. Mathematical operations are performed.
4. A unique hash value is generated.
5. Hash is stored on blockchain.

**Features:**

• One-way cryptographic function
• Unique output generation
• High security
• Fast execution speed

**Advantages:**

• Prevents data tampering
• Ensures integrity verification
• Difficult to reverse-engineer
• Suitable for blockchain applications

**Blockchain Verification Algorithm**

Blockchain verification algorithms ensure decentralized and tamper-resistant storage of hash values. Once records are stored on blockchain, they cannot be modified without network consensus.

**Working Process:**

1. Hash value is generated.
2. Blockchain transaction is created.
3. Nodes validate transaction.
4. Hash is stored permanently.
5. Verification requests retrieve blockchain records.
6. Current hashes are compared with stored hashes.

## 4. EXPERIMENTAL RESULTS

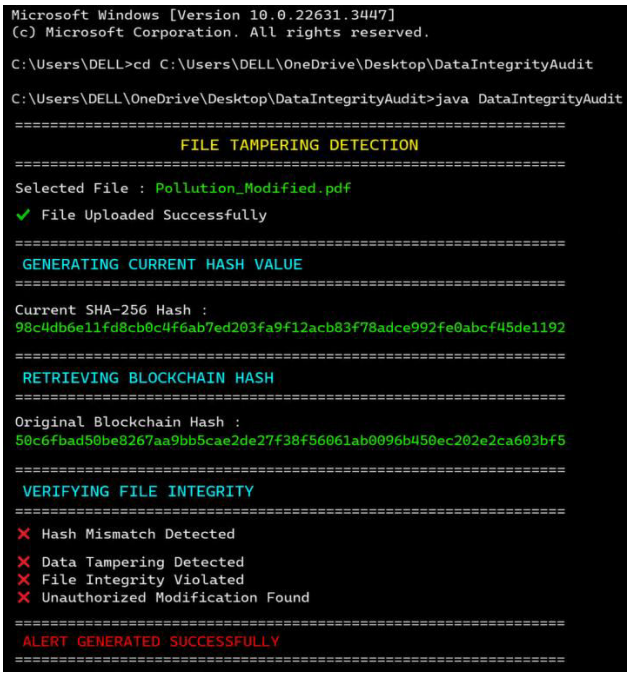
The proposed **Data Integrity Audit Scheme Based on Blockchain Expansion Technology** was successfully implemented and tested using blockchain technology, SHA-256 hashing algorithms, and web-based integrity verification mechanisms. The system produced accurate and reliable results during file upload, blockchain transaction generation, integrity verification, and tampering detection processes. The developed application successfully generated unique SHA-256 hash values for uploaded files and stored them securely on the Ethereum blockchain network. During testing, the system accurately verified whether files were modified by comparing current hash values with the original blockchain records. If the hash values matched, the system confirmed that the file remained secure and unmodified. If the hash values differed, the system immediately detected unauthorized modifications and displayed tampering alerts.

The frontend interface provided a simple and interactive environment for users to upload files, perform verification, and monitor integrity results. Backend modules developed using Node.js and Express.js efficiently handled blockchain communication, file processing, and hash generation operations.

The blockchain-based decentralized architecture successfully eliminated dependency on third-party auditors and improved transparency, reliability, and security of integrity verification. Experimental testing confirmed that blockchain records remained immutable and tamper-resistant throughout all operations.

### 4.1 IMPLEMENTATION OUTPUT

**1.** The implementation output confirms that the proposed blockchain auditing framework performs all operations successfully without errors. The system correctly processes uploaded files, generates SHA hash values, stores blockchain transaction records, and verifies integrity in real time



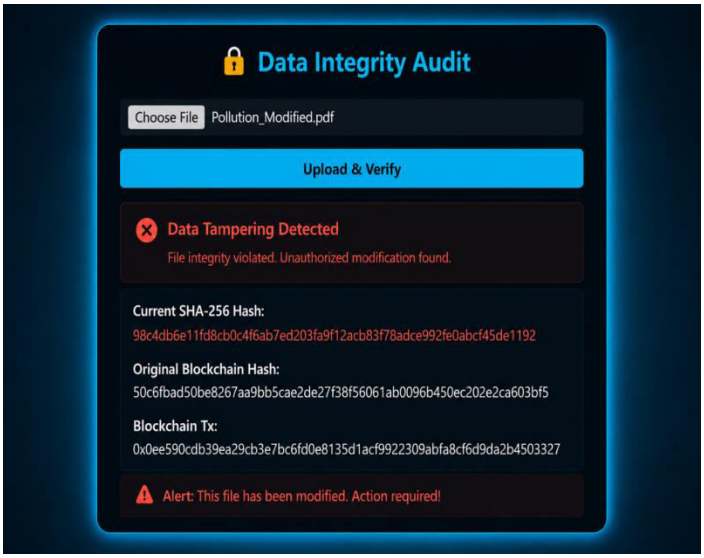



**Fig:2 Data Integrity Verification Processing Screen**

### 4.2 TAMPERING DETECTION OUTPUT

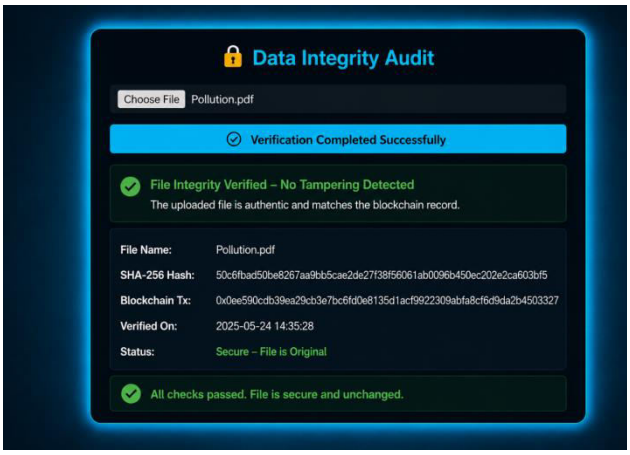



**Fig: 3 Successful Blockchain Integrity Verification Output**

## 5. CONCLUSION

The proposed Data Integrity Audit Scheme Based on Blockchain Expansion Technology successfully provides a secure, decentralized, and transparent framework for integrity verification in cloud-based environments. The developed system effectively combines blockchain technology and SHA-256 cryptographic hashing algorithms to ensure that stored files remain authentic, secure, and tamper-free throughout their lifecycle.

The implementation results demonstrate that the system accurately generates unique hash values for uploaded files and securely stores them on the blockchain network. During integrity verification, the generated hash values are compared with blockchain-stored records to identify unauthorized modifications. If any mismatch occurs, the system immediately detects tampering and generates alerts, thereby improving data security and reliability.

The decentralized blockchain architecture eliminates dependency on centralized third-party auditors and prevents unauthorized manipulation of integrity records. Blockchain technology provides immutability, transparency, fault tolerance, and secure transaction management, making the proposed framework highly suitable for modern cloud storage applications.

The frontend interface developed using HTML, CSS, and Bootstrap provides an interactive and user-friendly environment for file upload, verification, and monitoring operations. Backend technologies such as Node.js and Express.js efficiently manage blockchain communication, cryptographic operations, and real-time verification processes.

Experimental results confirm that the proposed framework improves integrity verification accuracy, operational efficiency, system reliability, and security compared to traditional centralized auditing systems. The implemented solution successfully reduces privacy risks, enhances transparency, and provides secure decentralized auditing suitable for real-world applications.

The proposed system can be effectively used in cloud storage platforms, banking systems, healthcare applications, government record management, legal document verification, educational systems, and other security-sensitive environments where maintaining data integrity is critically important.

## 6. FUTURE SCOPE

Although the proposed system provides secure blockchain-based integrity verification, several enhancements can be incorporated in future work to improve functionality, scalability, performance, and security. Future developments may include the integration of Artificial Intelligence (AI) and Machine Learning (ML) techniques for intelligent threat detection, anomaly prediction, and real-time security monitoring to identify suspicious activities before data tampering occurs. The framework can also be extended to support multi-cloud environments for distributed integrity auditing, thereby improving scalability, fault tolerance, data availability, and cloud security. Real-time notification systems using email alerts, SMS services, and mobile applications can further enhance user awareness and enable faster responses to security incidents. Additionally, advanced blockchain platforms such as Hyperledger Fabric, Polygon, and private blockchain networks can be utilized to achieve faster transaction processing,

reduced operational costs, and enterprise-level security. The integration of decentralized storage solutions such as InterPlanetary File System (IPFS) can improve decentralization, fault tolerance, and secure data availability while reducing dependence on centralized systems. Furthermore, biometric authentication mechanisms, including fingerprint and facial recognition, can strengthen access control and user verification. Future implementations may also include Android and iOS mobile applications to support remote monitoring and integrity verification. Smart contracts can be integrated to automate auditing and verification processes, reducing manual effort while improving transparency and efficiency. Support for big data environments can further enhance enterprise scalability and high-volume data processing capabilities. Finally, advanced cybersecurity techniques such as intrusion detection systems, zero-trust architectures, and enhanced encryption methods can be incorporated to strengthen security, privacy protection, and attack prevention mechanisms..

**REFERENCES**

1. Blockchain BasicsDaniel Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, Apress Publications, 2017.

2. Mastering BlockchainImran Bashir, Mastering Blockchain, Packt Publishing Ltd., 2020.

3. Cryptography and Network SecurityWilliam Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education, 2017.

4. Blockchain TechnologyChandramouli Subramanian, Blockchain Technology, Universities Press, 2021.

5. Data Communications and NetworkingBehrouz A. Forouzan, Data Communications and Networking, McGraw Hill Education, 2019.

6. Cloud ComputingRajkumar Buyya, Cloud Computing: Principles and Paradigms, Wiley Publications, 2018.

7. IEEEIEEE Research Papers on Blockchain-Based Data Integrity Verification Systems.

8. SpringerSpringer Journals on Blockchain Security and Cloud Data Auditing.

9. ElsevierElsevier Publications on Cryptography and Secure Cloud Computing.

10. International Journal of Advanced Computer Science and ApplicationsResearch Articles on Blockchain-Based Integrity Auditing Systems.

11. Ethereum Official Website

12. Node.js Official Website

13. MongoDB Official Website

14. SHA-256 Documentation

15. Blockchain Technology Tutorials

.

## Author Profiles

**Mrs. K. Pavani** Working as Assistant & Head of Department of MCA, in SRK Institute of technology in Vijayawada. She done with MCA, M. Tech in Computer Science. She has 10 years of Teachers experience in SRK Institute of technology, Enikepadu, Vijayawada ,NTR Distinct. Her area of interests includes Machine Learning with Python and DBMS.

**Mr.Jakkula Venkat Rayudu** Is An Mca Student In Department Of Computer Application In Srk Institute Of Technology , Enkeepadu, Vijayawada,NTR District .He Completed In Degree(Bsc Computers) Sir C R Reddy College Eluru