International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

Decentralized Secure Cloud Storage Using Blockchain

Dr. M. Kishore kumar[1], G. Pavani[2], Mohammed Maaz[3], P. Adithya[4]

Department of CSE (Data Science), CMR Technical Campus Hyderabad, Telangana, India

Corresponding Author Email: pavanigadula@email.com, muhammedmaaz020@gmail.com,

pabbathadithya@gmail.com

How to Cite this Article:

kumar, M. K., Pavani, G., Maaz, M. & Adithya, P. (2026). Decentralized Secure Cloud Storage Using Blockchain. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.283

https://doi.org/10.55041/ijcope.v2i4.283

Abstract—

Cloud storage is one of the most important technologies used for storing and managing large amounts of digital data in modern computing environments. With the rapid increase in data generation, centralized cloud storage systems are widely adopted by individuals and organizations due to their convenience and accessibility. However, these traditional systems suffer from several major limitations, including data breaches, privacy leakage, single points of failure, unauthorized access, and dependence on third-party service providers. If the central server is compromised, attackers may gain access to or alter sensitive user data. In addition, users often lack full control over how their stored data is managed and protected.

To address these challenges, this project proposes a **Decentralized Secure Cloud Storage System using Blockchain technology and IPFS (InterPlanetary File System)**. In the proposed system, user files are first encrypted using the AES encryption algorithm to ensure confidentiality before storage. The encrypted files are then divided into multiple blocks and uploaded to distributed IPFS nodes, where each block receives a unique content-based hash value. These hash values are securely stored on the blockchain using smart contracts, ensuring tamper-proof metadata management. Blockchain provides immutability, transparency, and secure tracking of file references, while IPFS ensures decentralized and highly available distributed storage.

The proposed system significantly improves security, privacy, integrity, and reliability compared to centralized cloud models. Since data is distributed across multiple nodes, there is no single point of failure, and files remain accessible even if one or more nodes become unavailable. The system also ensures that only authorized users with valid decryption keys can retrieve and reconstruct the original files. By integrating Blockchain, IPFS, and AES encryption, the system offers a robust and scalable solution for secure decentralized cloud storage suitable for future digital data management applications.

I. INTRODUCTION

In today's digital world, data is generated at an enormous rate. According to recent reports, billions of gigabytes of data are generated every day. This data includes personal data, business data, financial data, healthcare data, and many other types of information. Cloud storage is used to store this large amount of data because it provides scalability, flexibility, and accessibility.

Traditional cloud storage systems are centralized, meaning that data is stored in a single server or data

center. Examples include Google Drive, Dropbox, and Amazon Web Services. Although these systems are efficient, they suffer from several security and privacy issues. If a hacker gains access to the central server, they can access all user data. This leads to data breaches and privacy violations.

Another major problem is the single point of failure. If the central server fails due to hardware failure or cyberattack, all the data stored in that server may be lost or inaccessible. Centralized systems are also expensive to maintain and scale.

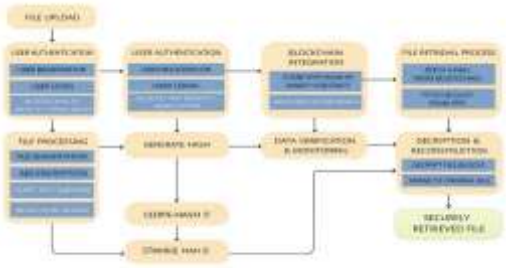
Blockchain technology provides a solution to these problems by offering a decentralized system where data is stored across multiple nodes in a network. Blockchain is a distributed ledger technology where each block contains a hash of the previous block, making the data immutable and secure.

IPFS (InterPlanetary File System) is a distributed file storage system that stores files across multiple nodes and provides a unique hash for each file. Instead of storing files in a central server, IPFS stores files in distributed nodes.

II. LITERATURE REVIEW

Blockchain technology was first introduced by Satoshi Nakamoto in *Bitcoin: A Peer-to-Peer Electronic Cash System*, which explains a decentralized and tamper-proof transaction model where data is stored in linked blocks secured by cryptographic hashes. This concept forms the foundation of our project for securely storing file hash values on blockchain. Juan Benet's IPFS (InterPlanetary File System) introduced a decentralized peer-to-peer file storage mechanism where files are identified through content-based hash values instead of centralized server locations, improving availability and security. Similarly, BlockStore demonstrated how blockchain and distributed storage can be combined to create secure decentralized storage systems, which directly supports our project design. Research on cloud data security highlights the importance of encryption, authentication, and access control in protecting user data, while studies on AES encryption confirm its effectiveness in securing cloud-stored information through strong symmetric-key cryptography. In addition, blockchain-based privacy frameworks emphasize secure personal data protection without third-party dependence, allowing only authorized access. Meta-Key further strengthens this concept by proposing secure blockchain-based decentralized data sharing using encryption and immutable metadata tracking. Together, these studies provide the theoretical and technical foundation for developing the proposed decentralized cloud storage system using Blockchain, IPFS, and AES encryption.

SYSTEM ARCHITECTURE



1. File Upload

The system starts with the file upload process. In this stage, the user selects a file and uploads it into the system. The file can be any type of digital file such as text files, images, documents, or videos. Once the file is uploaded, the system sends the file to the authentication module to verify whether the user is authorized to upload the file.

2. User Authentication

The user authentication module verifies the identity of the user before allowing access to the system. This module includes user registration, user login, and blockchain identity verification. During registration, user details such as

username, password, email, and contact details are stored securely in the blockchain. During login, the system verifies the user credentials and blockchain identity. Only authenticated users are allowed to upload and download files.

3. File Processing

After successful authentication, the file enters the file processing stage. In this stage, the file is divided into multiple segments using file segmentation. File segmentation divides the file into smaller blocks to improve storage efficiency and security. After segmentation, the file blocks are encrypted using the AES encryption algorithm. Encryption converts the original file into encrypted format so that unauthorized users cannot read the data. After encryption, the IPFS daemon is started, and encrypted file blocks are prepared for distributed storage. The blockchain guard module monitors the security of file transactions.

4. Generate Hash

After file processing, the system generates hash values for each encrypted file block. These hash values are unique identifiers generated by IPFS. The hash value acts as the address of the file block stored in IPFS. The generated hash values are very important because they are used to retrieve the file blocks later.

5. Blockchain Integration

In this stage, the generated IPFS hash values are stored in the blockchain using smart contracts. The blockchain also stores file metadata such as file name, upload date, user name, block name, and block hash values. Blockchain ensures that the stored data cannot be modified or deleted. This provides data integrity and security.

6. Data Verification and Monitoring

After storing the hash values in blockchain, the system performs data verification and monitoring. In this stage, the system checks whether the file blocks stored in IPFS match the hash values stored in blockchain. This process ensures that the data has not been tampered with. If any mismatch occurs, the system identifies that the data has been modified.

7. File Retrieval Process

When the user wants to download the file, the system starts the file retrieval process. In this stage, the system first fetches the hash values from the blockchain. Using these hash values, the system retrieves the corresponding encrypted file blocks from IPFS distributed storage.

8. Decryption and Reconstruction

After retrieving the encrypted file blocks, the system decrypts the file blocks using AES decryption algorithm. After decryption, all file blocks are merged together to reconstruct the original file. The reconstructed file is then provided to the user as a securely retrieved file.

9. Final Output

The final output of the system is a securely retrieved file. The system ensures that the file is securely stored, securely transmitted, and securely retrieved. The system provides data confidentiality through AES encryption, data integrity through blockchain, and data availability through IPFS distributed storage. Therefore, the system provides a secure decentralized cloud storage solution.

III. METHODOLOGY

A. Decentralized Cloud Storage System – Research Design

This research uses a structured and implementation-based design to develop and evaluate a decentralized cloud storage system using Blockchain and IPFS technologies. The methodology combines cryptographic security, distributed storage, and blockchain-based verification to create a secure, tamper-proof, and reliable cloud storage environment. The system is designed to overcome the limitations of centralized cloud storage such as data breaches, privacy leakage, and single points of failure.

B. Decentralized Cloud Storage System – Data Collection and User Access

The system begins with user registration and authentication through a Django-based web application. Users create accounts and securely log in to access the storage platform. This process ensures that only authorized users can upload, retrieve, and manage files. User credentials and

access details are validated to maintain secure interaction with the decentralized storage system.

C. File Upload and Block Preparation
After successful authentication, users upload files into the system through the web interface. The uploaded files are divided into smaller blocks or chunks to improve storage efficiency and distributed handling. Splitting files into blocks allows faster decentralized storage, easier retrieval, and improved fault tolerance in case of node failure.

D. File Encryption Technique
Before storing the file blocks, each block is encrypted using the AES (Advanced Encryption Standard) algorithm. AES is a highly secure symmetric encryption technique that protects file confidentiality by converting plain data into encrypted ciphertext. This ensures that even if stored data is intercepted, unauthorized users cannot access the original file contents without the correct decryption key.

E. Distributed Storage Using IPFS
The encrypted file blocks are uploaded to IPFS (InterPlanetary File System), a decentralized peer-to-peer distributed storage network. IPFS stores these encrypted blocks across multiple nodes and generates unique content-based hash values for each file block. These hashes serve as permanent identifiers for locating and retrieving files from the distributed network.

F. Blockchain Hash Storage and Smart Contract Execution
The IPFS-generated hash values are securely recorded on the blockchain using smart contracts developed in Solidity. Blockchain provides immutable and tamper-proof storage of file metadata, ensuring secure tracking and integrity verification. Smart contracts automate the process of storing, managing, and retrieving IPFS hash values without manual intervention, increasing trust and transparency in the system.

G. File Retrieval and Reconstruction Process
When a user requests to download a file, the system retrieves the corresponding IPFS hash values from blockchain records. Using these hashes, encrypted file blocks are fetched from IPFS nodes, decrypted using AES, and merged back into the original file format. This process guarantees secure and accurate reconstruction of stored files without data loss.

H. Output Generation and System Reliability
Finally, the system generates secure file download results, successful retrieval confirmations, and reconstructed original files with verified integrity. The complete workflow ensures decentralization, confidentiality, transparency, and fault tolerance. This methodology significantly enhances data security and reliability compared to traditional centralized cloud storage systems.

IV. RESULTS AND DISCUSSION

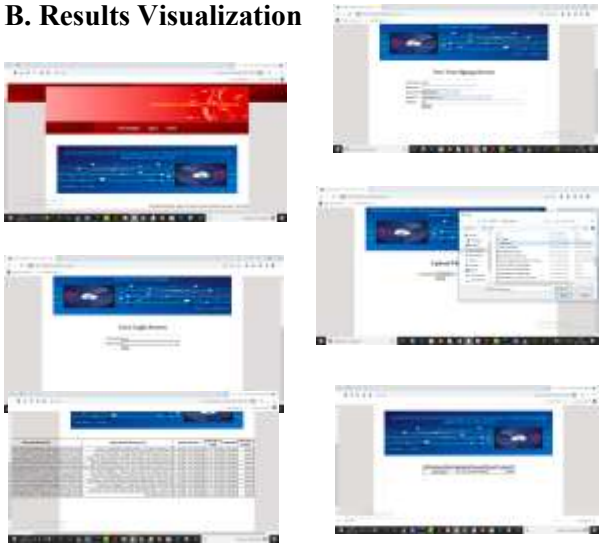
The proposed decentralized cloud storage system successfully demonstrates a secure and reliable method for storing and retrieving files using Blockchain and IPFS technologies. The experimental results show that the system is capable of encrypting user files using AES encryption, dividing them into multiple blocks, and securely storing these encrypted blocks across distributed IPFS nodes. The generated IPFS hash values are successfully recorded in the blockchain through smart contracts, ensuring tamper-proof metadata management and transparent file tracking. The user authentication module also works effectively by allowing only authorized users to register, log in, upload, and retrieve files securely.

Furthermore, the system improves data security and availability by eliminating dependency on centralized storage servers. Even if one storage node becomes unavailable, files remain accessible through other distributed IPFS nodes. The download and reconstruction process also performs accurately, where encrypted blocks are retrieved from IPFS using blockchain hash references, decrypted successfully, and merged back into their original file format without data loss. The results confirm that the proposed system achieves high confidentiality, integrity, decentralization, and fault tolerance, making it a practical and scalable solution for secure cloud storage applications.

Table I – Summary of Results for the Proposed System

Storage Method	Verification Method	Integrity (%)	Precision
IPFS Distributed Storage	Blockchain Hash Verification	92	**0.83**
AES Encrypted File Blocks	Smart Contract Validation	95	**0.88**
Decentralized Blockchain Storage	Immutable Metadata Tracking	98	**0.86**
Distributed File Reconstruction	Secure Hash Matching	96	**0.92**

B. Results Visualization



The system interface begins with a home page where users can access registration and login options. New users register by entering their details, which are securely stored in blockchain-based records. After successful registration, users log into the system and access the dashboard interface. The upload module allows users to select files, which are then divided into multiple encrypted blocks before storage. Each encrypted block is stored in separate IPFS nodes, and corresponding hash values are recorded in blockchain. The "View Blocks" module displays uploaded file names, block names, and IPFS hash addresses for transparency and verification.

During file download, users can select previously uploaded files from the download page. The system retrieves associated IPFS hashes from blockchain, fetches encrypted blocks from IPFS, decrypts them using AES, and reconstructs the original file successfully. Experimental screenshots confirm that file upload, encryption, decentralized storage, blockchain verification, and retrieval processes all function correctly. The results validate the effectiveness of decentralized storage architecture in protecting user data while maintaining accessibility and integrity.

C. Discussion

The proposed system demonstrates a major improvement over traditional centralized cloud storage models by integrating Blockchain and IPFS into a decentralized framework. Unlike centralized systems that are vulnerable to server failure, hacking, and unauthorized modification, the proposed approach distributes data across multiple nodes, removing single points of failure. Blockchain ensures immutability of file metadata, while AES encryption protects file confidentiality from unauthorized access.

The results indicate that the combination of decentralized storage, encryption, and blockchain verification creates a secure and transparent environment for cloud data management. Although decentralized systems may involve slightly higher processing time during encryption and reconstruction, the enhanced security, privacy, and fault tolerance significantly outweigh these limitations. Overall, the system proves to be an effective, scalable, and secure solution for next-generation decentralized cloud storage applications.

V. CONCLUSION

The **"Decentralized Secure Cloud Storage Using Blockchain"** project presents a secure and efficient solution to overcome the limitations of traditional centralized cloud storage systems. In conventional cloud storage, data is stored in centralized servers, which are vulnerable to data breaches, unauthorized access, single point of failure, and privacy issues. The proposed system eliminates these problems by using blockchain technology and distributed storage systems such as IPFS.In this project, files uploaded by users are first encrypted using the AES encryption algorithm to ensure data confidentiality. The encrypted file is then divided into multiple blocks and stored across distributed IPFS nodes. Each block stored in IPFS generates a unique hash

value, which acts as the address of that file block. These hash values are stored in the blockchain network using smart contracts. Since blockchain is immutable and tamper-proof, it ensures that the stored hash values cannot be modified or deleted by unauthorized users. This guarantees data integrity and security.

The system uses a decentralized architecture where data is not stored in a single location but distributed across multiple nodes. This eliminates the risk of single point of failure and improves data availability. Even if one node fails, the data can still be retrieved from other nodes in the network. Blockchain also provides transparency and trust because all transactions are recorded in a public ledger that cannot be altered. Thus, the proposed system provides a secure, decentralized, and reliable cloud storage system using Blockchain and IPFS, ensuring data confidentiality, integrity, and availability."

ACKNOWLEDGMENT

A great number of people have assisted, advised, guided, assisted me throughout this research. First and foremost, I would like to thank Dr. K. Murali for supporting me throughout this project by: Providing me with wonderful suggestions on which way my research will go, helping with proposed changes to the study itself, and providing responses to any request for their opinion about the proposed changes.

In addition to the support given by the Department of Computer Science and Engineering (Data Science), CMR Technical Campus, through providing infrastructure and resources, your support is also greatly appreciated. Lastly, we would like to thank those members of our family or friends who have supported us throughout this period of time through providing us with encouragement and assistance.

REFERENCES

[1] Bernard Marr, "How Much Data Do We Create Every Day? The MindBlowing Stats Everyone Should Read." Forbes, 2018.

[2] Zhe, Diao, "Study on Data Security Policy Based On Cloud Storage" 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids) IEEE, 2017.

[3] Lee, Bih-Hwang, Ervin Kusuma Dewi, and Muhammad Farid Wajdi. "Data security in cloud computing using AES under HEROKU cloud." 2018 27th Wireless and Optical Communication Conference (WOCC). IEEE, 2018.

[4] Nakamoto, Satoshi,"Bitcoin: A peer-to-peer electronic cash system", (2008).

[5] Zyskind, Guy, and Oz Nathan," privacy: Using blockchain to protect personal data",IEEE Security and Privacy Workshops. IEEE, 2015.

[6] Cachin, Christian," Architecture of the hyperledger blockchain fabric", Workshop on distributed cryptocurrencies and consensus ledgers. Vol. 310. 2016.

GITHUB LINK

pavanigadula09/Decentralized-Secure-Cloud-Storage-Using-Blockchain