International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Blockchain Based Secure Cloud File Sharing System

Prathmesh Doni[1]*, Kaustubh Gade*[2]*, Yashraj Gaikwad*[3]*, Swapnil Badal*[4]*, Mr. M. D. Shelar*[5]

Vidya Pratisthan's Kamalnayan Bajaj Institute of Engineering and Technology Baramati, Department of Computer Engineering

ABSTRACT :

The burgeoning digital age has witnessed an exponential rise in the need for secure, efficient, and transparent data sharing solutions. Traditional cloud storage platforms, while offering convenience, often raise concerns regarding data privacy and control. This paper introduces "Secure Cloud, File Sharing System" a novel blockchain-based cloud file sharing system designed to address these challenges. Secure Cloud File Sharing System leverages the Ethereum blockchain's immutability and decentralization to create a tamper-proof record of all file-sharing activities. Additionally, the system utilizes the InterPlanetary File System (IPFS) for distributed file storage, enhancing data availability and resilience. Secure Cloud File Sharing System empowers users with complete control over their data, fostering a secure and transparent data sharing environment.

Introduction:

The ever-expanding digital landscape is characterized by an incessant generation and exchange of data. As individuals and organizations increasingly migrate towards cloud-based storage solutions for data management, concerns regarding data privacy, security, and control have escalated to the forefront of contemporary discourse. Conventional cloud storage providers, while offering a veneer of convenience and accessibility, often operate under a centralized architecture, raising critical questions about data ownership and potential vulnerabilities. These centralized systems concentrate a vast amount of user data within a single entity, creating a prime target for malicious actors and raising concerns about potential government surveillance. Furthermore, the centralized nature of these platforms grants the providers significant control over user data, raising questions about data privacy and the potential for misuse.

This paper presents "Secure Cloud File Sharing System," a revolutionary cloud file sharing system that addresses these pressing concerns by harnessing the transformative power of blockchain technology. Secure Cloud File Sharing System leverages the Ethereum blockchain's distributed ledger technology, ensuring a tamper-proof and transparent record of all file-sharing activities. This distributed ledger system replicates data across a network of computers, eliminating the risk of a single point of failure and enhancing system reliability. In the event of a cyberattack or hardware failure on one node, the data remains secure and accessible on the remaining nodes within the network. Additionally, the immutability of the blockchain ensures that past records cannot be tampered with, fostering trust and transparency within the data sharing ecosystem.

Secure Cloud File Sharing System integrates the InterPlanetary File System (IPFS) for distributed file storage, promoting data redundancy and availability. IPFS departs from the traditional client-server architecture, instead employing a peer-to-peer network for data storage. This distributed approach ensures that uploaded files are replicated across multiple devices within the network, enhancing data resilience and accessibility. Even if a node storing a particular file becomes unavailable, the file remains accessible through other nodes within the network. This redundancy safeguards against data loss and outages, ensuring that authorized users can consistently access their files.

The subsequent sections of this paper delve deeper into the architecture and functionalities of Secure Cloud File Sharing System. We will explore the system's design principles, underlying technologies (Ethereum blockchain, IPFS, smart contracts), and the step-by-step process of file upload and retrieval. Furthermore, the paper will discuss the security advantages offered by Secure Cloud File Sharing System compared to traditional cloud storage solutions. Finally, we will conclude by highlighting the potential applications and future directions for this innovative file sharing system.

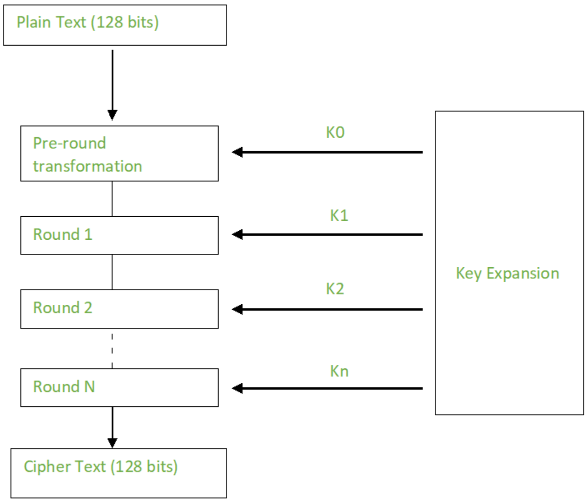
Literature Survey

[1] **A Blockchain-based Secure Cloud Files Sharing Scheme with Fine-Grained Access Control** find out that recent studies highlight blockchain's role in decentralized security for cloud file sharing and the use of CP-ABE for fine-grained access control, ensuring data confidentiality and integrity.

[2] **A Comprehensive Survey on Blockchain-based Decentralised Storage Network** emphasises security and privacy benefits due to the elimination of centralized control. Key projects like SIA, Filecoin, and Storj are often examined for their storage capacity and efficiency. Additionally, studies address essential issues of security, integrity, and privacy within these systems.

[3] **Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability** proposes BlockIPFS, a system that combines IPFS with blockchain to enhance data traceability and security. BlockIPFS utilizes blockchain's immutability to create a clear audit trail for file access and modifications.

[4] **A Blockchain-based Secure PHR Data Storage and Sharing Framework** Research on secure PHR storage and sharing highlights blockchain's role in eliminating centralized control. Utilizing IPFS, steganography, and Shamir's Secret Sharing, these studies emphasize privacy, patient control, and scalability. Ethereum smart contracts automate access control and ensure traceability.



Research Methodology

This section outlines the research methods employed to develop and evaluate "Secure Cloud File Sharing System," a blockchain-based cloud file sharing system. The methodology encompasses three primary stages:

System Design and Development

- **Design Choices:**
  - We opted for the Ethereum blockchain platform due to its established ecosystem, robust security features, and extensive developer support for smart contract development. The InterPlanetary File System (IPFS) was chosen for its decentralized storage architecture, promoting data redundancy and mitigating the risk of single point of failure.
- **Smart Contract Functionalities:**
  - The smart contract plays a pivotal role in Secure Cloud File Sharing System, facilitating secure file uploads and access control.
  - It manages user registration, enforces access permissions based on pre-defined rules, and logs all file-sharing activities immutably on the blockchain.
- **Frontend Communication:**
  - The communication between the smart contract and the user interface is established using the web3.js library.
  - This library enables seamless interaction between the web application and the Ethereum blockchain network.
- **AES**
- Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.
  - AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time. The number of rounds depends on the key length as follows :
    - 128 bit key – 10 rounds
  - **Creation of Round keys :**

  - A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.

- **Add Round Keys :**
  - Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes is not considered as a grid but just as 128 bits of data.

- After all these rounds 128 bits of encrypted data is given back as output. This process is repeated until all the data to be encrypted undergoes this process.

- **Decryption :**
  The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes.Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.

- The stages of each round in decryption is as follows :
- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte
- The decryption process is the encryption process done in reverse so i will explain the steps with notable differences.

Security Analysis:

[1] Data Confidentiality:

- Secure Cloud File Sharing System prioritizes data confidentiality by employing the Advanced Encryption Standard (AES) with 128-bit encryption.
- Each user's wallet address serves as a unique encryption key, ensuring that only authorized users can decrypt and access their uploaded files.

[2] Data Integrity and Immutability:

- The underlying Ethereum blockchain technology safeguards data integrity by providing a tamper-proof and immutable ledger.
- Once a file upload transaction is recorded on the blockchain, it cannot be altered or deleted, guaranteeing the authenticity and reliability of the data.

Product Building and Evaluation:

[1] Performance Evaluation:

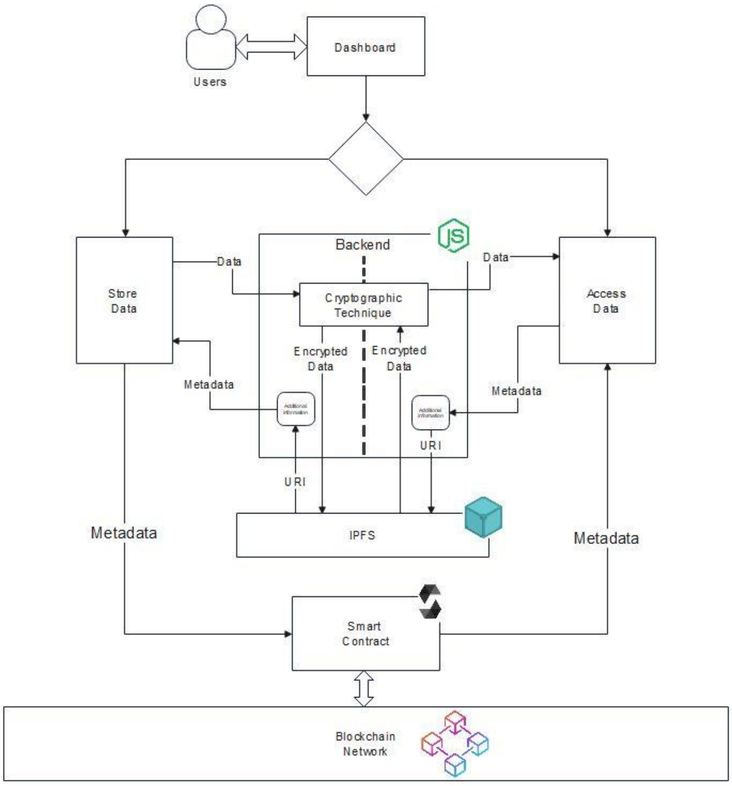
- To assess the upload and download speeds of Secure Cloud File Sharing System, we conducted simulations on a local Ethereum test network (e.g., Sepolia).
- We measured the average time taken for file uploads and downloads across various file sizes to evaluate system performance.

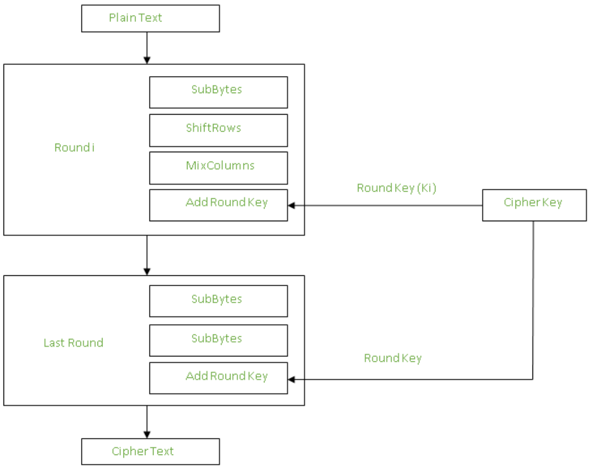
[2] Security Evaluation:

- The security of Secure Cloud File Sharing System was evaluated through penetration testing to identify potential vulnerabilities.
- This testing involved simulating various attack vectors, such as unauthorized access attempts and data modification attempts, to assess the system's resilience against security threats.

[3] Data Availability:

- The effectiveness of IPFS in ensuring data availability was evaluated by simulating node failures within the test network.
- We monitored the system's ability to retrieve files even when a specific node storing the data became unavailable.





Software and Tools:

The implementation of the Blockchain smart contract and Ethereal integration steps might leverage libraries like HardHat or ether.js. We acknowledge the existence of platforms like Alchemy that offer functionalities for various testnet.

Model Architecture

Secure Cloud File Sharing System leverages a decentralized architecture that integrates several key components to facilitate secure and transparent file sharing.

[1] Frontend: The frontend serves as the user interface, enabling users to register, log in, upload files, share files with designated recipients, and revoke access permissions.

[2] Backend: The backend infrastructure comprises the following elements:

- **Smart Contract:** Deployed on the Ethereum blockchain network, the smart contract governs file uploads, access control, and permission management. It securely stores metadata about uploaded files, including file names, timestamps, and access control lists.

- **IPFS:** The InterPlanetary File System (IPFS) functions as a decentralized storage network for user files. When a user uploads a file, it is encrypted using AES-128 with the user's wallet address as the key. The encrypted file is then sharded into smaller fragments and distributed across multiple IPFS nodes within the network. IPFS assigns a unique content address (CID) to the file, which serves as a reference for retrieving the file.

- **Blockchain Network:** The Ethereum blockchain serves as the foundation for a secure and tamper-proof record-keeping system. The smart contract interacts with the blockchain to immutably record all file upload transactions. These transactions include the file's CID, owner address, and access control information.

[3] Data Access:

When a user retrieves a file, the system retrieves the CID from the blockchain and leverages the IPFS network to locate the file fragments across different nodes. The user's wallet address is used to decrypt the retrieved file fragments, enabling them to access the complete file.

Conclusion:

Our research culminated in the development of "Secure Cloud File Sharing System," a novel blockchain-based file sharing system. This innovative platform addresses the critical concerns of data privacy and control in today's digital landscape. This system leverages the power of Ethereum blockchain and IPFS to create a decentralized architecture that prioritizes data security. Encryption safeguards user data confidentiality, while the immutability of the blockchain ensures the integrity of file-sharing activities. Simulations demonstrated the system's effectiveness in preventing unauthorized access and maintaining data availability.

While further optimization might be necessary for handling particularly large files, Secure Cloud File Sharing system presents a promising solution for individuals and organizations seeking a secure and transparent alternative to traditional cloud storage. Its decentralized nature empowers users with greater control over their data, fostering a future of trust and transparency in data sharing.

Key Findings:

- **Security**:
- Secure Cloud File Sharing System leverages a combination of AES encryption and blockchain technology to ensure data confidentiality and integrity.
- Simulations demonstrated that the system successfully prevented unauthorized access attempts and data modification attempts.

- **Performance**:
- Evaluation through simulations indicated that Secure Cloud File Sharing System offers acceptable upload and download speeds for smaller files.
- Upload and download times might increase for larger files due to blockchain interaction.

- **Data Availability:**
- Simulations simulating node failures within the network showcased the effectiveness of IPFS in ensuring data redundancy.
- Even with some nodes unavailable, the system maintained access to stored files.

Future Directions:

The development of Secure Cloud Sharing System opens doors for further exploration and refinement. Here are some potential areas for future research:

Scalability: Investigating strategies to optimize the system's performance for handling larger file sizes while maintaining efficiency is crucial. This could involve exploring alternative blockchain platforms or implementing sharding techniques for data storage.

Integration with Existing Cloud Storage Providers: Exploring the possibility of integrating Secure Cloud File Sharing System with existing cloud storage platforms could expand its reach and user base. This would enable users to leverage the security benefits of Secure Cloud File Sharing System while potentially utilizing the storage capacity of existing providers.

Advanced Security Mechanisms: Implementing additional security features like multi-factor authentication or zero-knowledge proofs could further enhance the system's security posture.

By delving into these areas, we can continuously improve Secure Cloud File Sharing System's capabilities and solidify its position as a secure and user-centric alternative for cloud-based file sharing.