International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Blockchain Based Cloud File Sharing System

Ramesh Kumar Yadav
Department of Computer Science & Engineering
Faculty of Engineering & Technology
JAIN (Deemed -to- be) University
Bangalore, India
21btrcm027@jainuniversity.ac.in

Varun N.V
Department of Computer Science & Engineering
Faculty of Engineering & Technology
JAIN (Deemed -to- be) University Bangalore, India
21btrcm012@jainuniversity.ac.in

Dr. Raja Parveen N
Department of Computer Science & Engineering
Faculty of Engineering & Technology
JAIN (Deemed -to- be) University
Bangalore, India
p.raja@jainuniversity.ac.in

ABSTRACT

Although blockchain is excellent for decentralized transaction recording, it has certain drawbacks when it comes to storing big files or documents. Decentralized storage systems have been created to effectively manage greater volumes of data in order to address this problem. A distributed system called blockchain makes sure that transactions are safe and clear. To enhance data sharing, some strategies have looked into combining blockchain with other technologies. However, relying solely on blockchain technology for safe file sharing has drawbacks. In this study, we present a secure file-sharing system that combines group key management and distributed access control. To make sure that only authorized users may access shared data, our system uses blockchain technology to enforce control regulations. Depending on their preferences, users can join existing groups or form new ones. Although access control techniques are not inherent in typical blockchain networks, our solution efficiently regulates access restrictions, granting members access to only the files that belong to their approved groups. By protecting against unwanted access, guaranteeing data integrity, and keeping a clear transaction history, the system improves security. Access control is automated using smart contracts, which lessens the need for centralized authorities. Furthermore, file confidentiality is protected during transmission and storage using encryption mechanisms. Using blockchain technology, this method offers a scalable and effective way to share files securely on the cloud.

Keywords: Cloud, Blockchain, file sharing, Inter-Planetary File System (IPFS), access control, group key management

1. INTRODUCTION

Blockchain has become one of the most innovative technologies in recent years. It was first made public in 2008 and is commonly acknowledged as the basis for Bitcoin. Blockchain provides a novel means of enabling safe transactions between two people without the need for a centralized authority. Its immutability, which guards against data manipulation and maintains trust, is one of its main advantages.

Blockchain also offers a number of other advantages. Because of its decentralized structure, no one organization has total authority over the system. Through the use of cryptographic techniques, transactions are safely connected, transparent, verifiable, and

impervious to corruption. This improves dependability and trust in a variety of applications.

The potential of blockchain technology to offer decentralized, transparent, and safe solutions has drawn a lot of interest. Blockchain technology has been used in a number of attempts to create effective file-sharing networks. One method, for instance, used a re-encryption token to handle keys and developed a blockchain-based storage system for exchanging IoT data. When an authorized user's access is canceled, this technique updates the encryption keys to stop additional access. However, there is more computational cost because the data owner is solely responsible for the key encryption and update procedures.

A scalable and reliable file-sharing solution utilizing a distributed key management strategy and re-encryption mechanism was presented by another proposed system. This method protects against collusion attempts from revoked users while guaranteeing that numerous users can safely access data. However, because authorized users share a portion of the encryption key, key management duties are transferred to the users, raising the possibility of security breaches. There are certain restrictions and inefficiencies in the current schemes. In this work, a secure file-sharing system based on blockchain technology is introduced to improve computational overhead and lower security threats. We use group key management and a decentralized access control system to improve efficiency and security. To guarantee that only authorized users may access them, files are encrypted before being stored.

Blockchain also serves as a trackable and unchangeable ledger, logging file upload details to guard against data corruption and unwanted changes. Our technology makes use of blockchain's security and transparency capabilities to guarantee that only members of the selected group can access shared files. A safe and adaptable file-sharing environment is maintained by allowing users to start new groups or join ones that already exist. This is how the remainder of the paper is structured. The history of blockchain technology is covered in Section II. In Section III, the suggested secure file-sharing system is introduced, along with an explanation of how blockchain technology can be used to improve efficiency and security. In Section IV, the conclusion and next steps are finally discussed.

BACKGROUND

In this section, we describe the key technologies relevant to the proposed secure file-sharing system.

Blockchain

A blockchain is a distributed ledger in which nodes in the network that are involved keep the records. To guarantee integrity and security, these nodes validate transactions and encrypt them using cryptographic techniques.

A digital cryptocurrency created to offer a decentralized financial system; Bitcoin was the first successful application of blockchain technology. Because transaction records are kept on a distributed ledger and verified by network users, users can trade assets with trust. Transactions are added to the blockchain after verification, which makes them unchangeable and impenetrable.

Participants in the blockchain network, referred to as miners, use processing power to verify transactions. Miners receive cryptocurrency in exchange for their labor as a reward. By preventing any one party from controlling transaction validation, this approach maintains the system's decentralization and credibility while guaranteeing consensus throughout the network.

Proof-of-work is introduced as a consensus technique to reach consensus inside the blockchain network. A series of transactions, data to track transaction history, and the solution to a mathematical challenge are usually included in a new block. Miners solve the puzzle through computational work. The block becomes valid once the puzzle has been solved and the answer has been entered.

Anyone in the blockchain network can take part in this process by figuring out the puzzle; they will receive transaction fees in exchange. While preserving security and decentralization, this proof-of-work approach makes sure the network comes to an agreement.

As previously stated, Bitcoin is a permission-less open blockchain. This makes it simple for anyone to join the network, initiate transactions, or take part in the consensus process as a client or miner. An further illustration of an open blockchain is Ethereum.

A consortium blockchain, on the other hand, differs in that a collection of approved nodes controls it. It is known as a permissioned blockchain since these nodes oversee the validation procedure and are pre-approved. One well-known example of a permissioned blockchain is Hyperledger. To ensure a controlled and reliable environment, a trusted central authority is needed to verify nodes who want to join the network, in contrast to permission-less blockchains.

Blockchain is a distributed ledger, as was previously said, and the records on the chain contain a collection of transactions as well as the data required to trace the transaction history. When it comes to directly storing huge files or documents on the blockchain, there are certain restrictions. Because the size of the data in each block is constrained, blockchain is effectively an expensive database for storing vast volumes of data.

In order to get around this restriction, a decentralized storage system is presented, in which big files are kept off the network and the blockchain acts as a transparent, safe ledger for monitoring file upload information. By fusing the immutability and transparency of blockchain technology with a more scalable and affordable storage solution, this method increases efficiency and enables safe file sharing.

Cloud

Cloud storage is the foundation for storing big files and documents in the framework of the suggested blockchain-based cloud file-sharing system. The technology is made to get over the drawbacks of conventional blockchain networks, where the little amount of space in each block makes it costly and ineffective to store vast amounts of data directly on the blockchain. In this concept, the actual file data is kept on a decentralized cloud storage platform, and the blockchain is utilized to secure transactions, guarantee integrity, and preserve metadata.

Because cloud storage is decentralized, files are dispersed among several network nodes. This method improves the storage system's scalability and robustness. Without depending on a server or central authority, every file is saved to guarantee high availability and ease of access. Redundancy is ensured by the distributed nature of cloud storage, which means that copies of the files are present on several nodes, ensuring data availability even in the event that some nodes fail.

This method incorporates blockchain technology to create a safe and unchangeable ledger. Blockchain keeps track of the files' metadata, transaction history, and access control rules rather than the actual files. The blockchain logs the transaction when a file is uploaded to the cloud, making the upload verifiable and impenetrable. The files' unique identifiers, which point to their separate locations on the decentralized cloud storage network, are likewise stored on the blockchain.

Additionally, the blockchain makes sure that only authorized individuals may access the files by enforcing access control regulations. Blockchain transactions are used to confirm each user's identity and authorization, adding an additional degree of security and responsibility. Only users who belong to a certain group are able to access files, guaranteeing that the files are safely shared inside the approved circles.

Decentralized cloud storage and the blockchain network work together to guarantee the efficiency and security of the file-sharing system. Decentralized cloud storage offers the scalability and affordability required to store big files, while blockchain ensures the integrity of transaction records and file metadata is preserved. By doing away with the requirement for expensive centralized servers, this hybrid solution lowers the overall cost of storage while increasing the system's resilience to failures.

This system offers a reliable, safe, and scalable solution for cloud-based file sharing by utilizing blockchain for transaction monitoring and security and cloud storage for effective file management. It gives users the freedom to post, save, and distribute files in a safe, decentralized setting while taking advantage of blockchain technology's transparency and immutability. This makes it the perfect choice for sectors that demand a high degree of data integrity and secrecy because it guarantees that all file-related operations are transparent, traceable, and secure.

PROPOSED SCHEME

We propose a permission-less blockchain-based safe file-sharing system. Any user can join the network and take part in transactions thanks to the permission-less blockchain. However, the file-sharing system may encounter possible permission problems because there isn't a reliable central authority. Our concept addresses this by introducing a distributed access control system and group key management, which effectively secures and manages permissions using blockchain technology.

Motivation

A distributed ledger called blockchain makes it possible to record transactions in a decentralized manner. However, due to memory limitations on nodes in the blockchain network, only transaction records—not big files—can be kept on the blockchain. We present a decentralized storage approach to overcome this constraint. Blockchain offers openness and security, but it doesn't completely take computing costs and security threats into consideration. This makes a secure and effective solution necessary. In this work, we present a permission-less blockchain-based secure file-sharing system that uses a distributed proxy approach to store group keys and access control policies.

System Model

The Owner, User, IPFS Proxy, IPFS Server, and Blockchain are the entities that make up the system model, as depicted in Figure 1. Every component is essential to the safe file-sharing system.

Owner

When a new group is created in the system, the owner is the first person to join it. As the original group member, the owner controls the access rules and has the authority to distribute files within the group. The owner has the power to decide who is allowed to join the group and view the files.

User

When a user joins a group, they can access the files that other group members have shared. Depending on the access policies established by the owner, the user is able to access and decrypt files in the group.

IPFS Proxy

When a new group is formed, the IPFS proxy creates a pair of group keys. To protect the privacy of the files uploaded by group members, files are encrypted using the group key. The mapping table, which houses the group members' public keys, is maintained by the IPFS proxy. The proxy ensures safe file access by encrypting the group key using the member's public key and sending it to the authorized member upon request for a file.

IPFS Server

The files that have been encrypted by the IPFS proxy are stored on the IPFS server. The IPFS server obtains and sends the encrypted file back to the user upon request from an authorized member. The IPFS server merely acts as storage; it does not decrypt the files.

Blockchain

Information about file uploads, such as the file's hash value and identifier, is stored on the blockchain. The immutable nature of the blockchain guarantees the preservation and unquestionable integrity of the file's ownership. The system uses the blockchain to monitor file sharing operations, guaranteeing that the file's history can be traced and that the contents has not been altered.

File sharing is protected by decentralized access control mechanisms, traceable, and secure thanks to this system concept.

Registration of the Owner:

The owner must first register at the IPFS proxy in order to create a new group in the connecting each group_id with the key lists of the users who have registered for the system, the IPFS proxy keeps track of a mapping table.

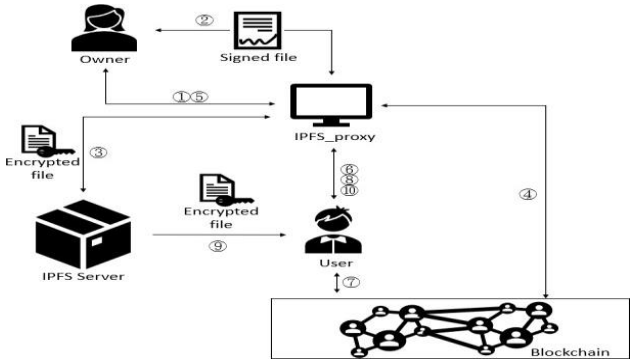

Figure 1. Overview of the proposed secure file sharing system

Work Flow

The following steps outline the Blockchain-Based Cloud File Sharing System's workflow:

File Signing and Uploading:

The file that is prepared for uploading is signed by the registered owner. The legitimacy of the signature is confirmed by the IPFS proxy. The IPFS proxy hashes the file and creates a file_hash to guarantee the file's integrity when the signature is verified as legitimate. The group key, which was previously produced by the IPFS proxy, is then used to encrypt the file. When the IPFS server receives this encrypted file, it confirms its storage by returning an IPFS_hash.

Storing File Information:

The IPFS proxy saves the file_hash, group_id, and user_id values on the blockchain after receiving the IPFS_hash. In the blockchain network, this data guarantees file traceability and verification.

Blockchain Transaction:

Next, a transaction is broadcast via the blockchain network. After receiving the transaction_id (trans_id), the IPFS proxy gives it back to the owner. The file's upload and blockchain registration are verified by this transaction identity.

Completion of File Uploading:

The uploading procedure is deemed finished once the trans_id is returned. The owner can now handle the uploaded file within the safe file sharing system and has a record of the transaction.

Figure 2 displays a sequence diagram for the file uploading procedure that describes how the owner, IPFS proxy, IPFS server, and blockchain network interact.

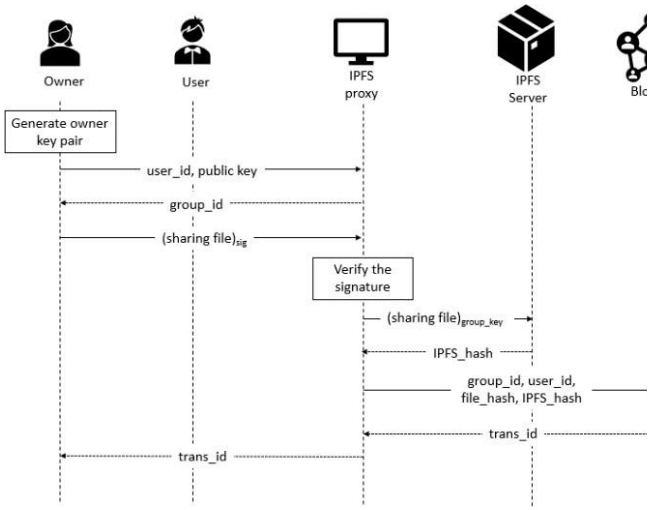

Figure 2. Sequence diagram for file uploading process

User Registration and Authorization:

A new user must first create a key pair (public and private keys) in order to access files associated with a particular group_id. After that, the user uploads their public key to the IPFS proxy along with their user_id and the assigned group_id. To access the files in the group, a new user must have permission from the group owner. The IPFS proxy updates the user's public key in the mapping table and completes the user registration procedure if the group owner gives permission.

Querying Transaction Data on Blockchain:

Using the transaction_id (trans_id), the user queries the blockchain for transaction data after being granted permission. The user signs the request to the IPFS proxy using the group_id, user_id, and IPFS_hash after receiving the transaction data, which consists of group_id, user_id, file_hash, and IPFS_hash. This guarantees that the user's request is genuine.

Verification and File Retrieval:

The IPFS proxy uses the IPFS_hash to query the IPFS server and confirms the user's identity. The user is subsequently sent the specified encrypted file by the IPFS server.

File Decryption and Key Wrapping:

Because the encrypted file is encrypted using the group key produced by the IPFS proxy, the user is unable to access it straight after receiving it. We provide a key wrapping method to solve this, in which one key encrypts another. Here, the user receives a key wrapping key from the IPFS proxy, which uses the user's public key to encrypt the group key. The group key is then obtained by the user using their private key to decrypt the key wrapping key. The user can use the group key to decrypt the file after obtaining it.

File Integrity Verification:

The user hashes the file after decrypting it and compares the outcome with the file_hash that was downloaded from the blockchain. The integrity of the file is checked to make sure it hasn't been altered if the hashes match.

Figure 3 displays the sequence diagram for the file download process, which shows how the user, IPFS proxy, IPFS server, and blockchain network interact. Now that the secure file sharing procedure is finished, only authorized users will be able to view and validate the files.

Access Control

Access control in the Blockchain-Based Cloud File Sharing System is largely managed via the IPFS proxy. It acts as a platform for people who want to sign up for the secure file sharing system to register and validate.

Following registration, the IPFS proxy stores a mapping table with the user's public key. A new group key is created for that group by the IPFS proxy upon a new owner's registration request. A symmetric key, such as AES-CBC, is used as the group key since symmetric cryptosystems are faster and more effective. Following that, as illustrated in Figure 4, this group key is kept in the mapping table with the owner's public key.

When a user wishes to join the same group, their public key is added to the mapping table for that particular group after it has been validated. Every group in the IPFS proxy has its own mapping table, which serves as the group's access control policy. This method offers a strong mechanism for controlling access control in the file sharing process by guaranteeing that only authorized users can access the files shared within each group.

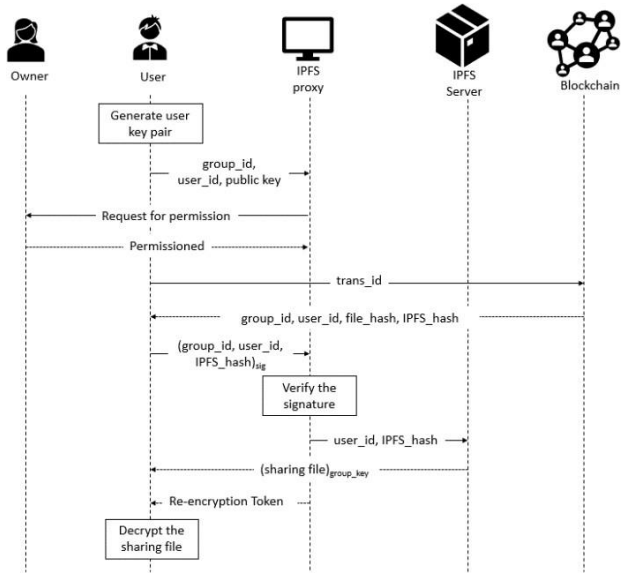

Figure 3. Sequence diagram for file downloading process

Revocation

The same group key is used to encrypt all shared files within the same group. The mechanism causes the IPFS proxy to create a new group key in order to replace the previous one in the event that a member is removed from a group. The new key has to be used to re-encrypt all group-related files on the blockchain and the IPFS server. These encrypted files' new IPFS hashes are added to the blockchain as a new transaction. The new group key, which is encrypted using the public key of the permitted users, will be distributed to all users—aside from the revoked member.The modified group key is used to encrypt the new files, preventing the revoked member from accessing any material in the future. A communication overhead proportional to O(n), where n is the number of users in the group, is involved in the revocation process.

Group Management

Users can join more than one group in our Blockchain-Based Cloud File Sharing System. For instance, as shown in Figure 4, Alice, Bob, and Carol are in Group 1, whereas Bob and Charlie are in Group 2. As a member of both groups, Bob asks for the IPFS proxy for the Group 1 key, which is encrypted using his public key, in order to access files in Group 1. Bob can decrypt and access the files from Group 1 once he has the key. In a similar manner, Bob can retrieve files from Group 2 by asking for the group's matching key.

Alice, on the other hand, can only access files from Group 1 because she and Bob are members of the same group. Bob has authority to read files from both groups, but Charlie can only access files from Group 2. Regardless of how many groups a user is a part of, the group management system makes sure that they are categorized according to the groups they are a part of. This guarantees effective file access management based on group memberships.

Security

The IPFS proxy is trusted in our Blockchain-Based Cloud File Sharing System, and users who successfully complete the registration process are regarded as trustworthy. However, because its data is available to everybody on the internet, the IPFS server and Blockchain are seen as unstable. Without the correct group key, unauthorized users are unable to decode the encrypted files, even though they can access the data from the IPFS server and Blockchain. The group's security in the file-sharing system is guaranteed by the IPFS proxy, which manages the access control settings.

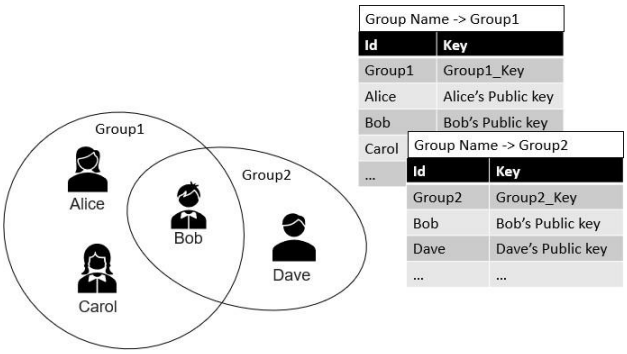

Figure 4. Group key management and the mapping table in the IPFS proxy

CONCLUSION AND FUTURE WORK

In this work, we propose a permission-less blockchain-based secure file-sharing system. Using a blockchain network, the system integrates a distributed access control and group key management mechanism. The integrity and security of the file-sharing system are guaranteed by the combination of a decentralized proxy and the blockchain network. Depending on their preferences, system users are allowed to start new groups or join ones that already exist. Our secure file-sharing system efficiently handles access control policies, even if the blockchain and cloud storage network lack built-in access control features. Only the files linked to the groups that users are permitted to join are accessible to them. We are now completing the implementation of our design, and in subsequent work, we intend to present the comprehensive performance outcomes to support our methodology.

REFERENCES

1. Nakamoto, Satoshi, and A. Bitcoin. "A peer-to-peer electronic cash system." Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf (2008).

2. Benet, Juan. "Ipfs-content addressed, versioned, file system." arXiv preprint arXiv:1407.3561 (2014).

3. Shafagh, Hossein, et al. "Towards blockchain-based auditable storage and sharing of IoT data." Proceedings of the 2017 on Cloud Computing Security Workshop. 2017.

4. Ateniese, Giuseppe, et al. "Improved proxy re-encryption schemes with applications to secure distributed storage." ACM Transactions on Information and System Security (TISSEC) 9.1 (2006): 1-30.

5. Cui, Shujie, Muhammad Rizwan Asghar, and Giovanni Russello. "Towards blockchain-based scalable and trustworthy file sharing." 2018 27th International Conference

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

7. Protocol Labs. Filecoin: A Decentralized Storage Network. Online: https://filecoin.io/filecoin.pdf, 2017.

8. Hartman, John H., Ian Murdock, and Tammo Spalink. "The Swarm scalable storage system." Proceedings. 19th IEEE International Conference on Distributed Computing Systems (Cat. No. 99CB37003). IEEE, 1999.

9. Dong, Changyu, Giovanni Russello, and Naranker Dulay. "Shared and searchable encrypted data for untrusted servers." Journal of Computer Security 19.3 (2011): 367-397.

10. Ethereum White-Paper. Online: https://github.com/ethereum/wiki/wiki/ White-Paper, 2019.