Journal of Information Systems Engineering and Management
2025, 10(16s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Secure File Sharing Using Blockchain and IPFS with Smart Contract-Based Access Control

Dr. Neeta P. Patil[1], Dr. Yogita D. Mane[2], Dr. Anil Vasoya[3], Akshay Agrawal[4], Sanketi Raut[5]
[1,3]*Associate Professor, Dept. of IT, Thakur College of Engg. and Tech., Mumbai, Maharashtra, India*
[2] *Associate Professor, Dept. of AI&DS, Thakur College of Engg. and Tech., Mumbai, Maharashtra, India*
[4,5] *Assistant Professor, Dept. of IT, Universal College of Engineering, Mumbai, Maharashtra, India*

ARTICLE INFO

Received: 04 Dec 2024

Revised: 25 Jan 2025

Accepted: 12 Feb 2025

ABSTRACT

With the growing demand for secure, decentralized file sharing solutions, this study presents a blockchain and IPFS-based framework for efficient data storage and access control. The proposed system leverages asymmetric encryption, smart contracts, and distributed access management to ensure confidentiality and integrity. The files are encrypted using AES-256 before they are stored in IPFS, and SHA-256 hashing is used to verify the content. Access control is guaranteed using blockchain-based policies, encrypting access keys and dynamic permissions to ensure that users can exchange files. An intelligent contract automates authentication, access and distribution of keys, minimizing dependence on centralized bodies. In addition, suppliers of storage facilities for an incentive mechanism reward the economy of economic and scalable storage. By using consensus mechanisms, such as proof of aspiration (POS) or proof of the authorities (POA), the system prevents unauthorized modifications and increases data security. This approach provides a reliable solution for organizations requiring controlled access to confidential data, with potential applications in the field of financial, health care and public sectors.

Keywords: Blockchain, IPFS, Node-Based-Storage, Cloud-Based-Storage, immutable, smart-contract

INTRODUCTION

The exponential boom of virtual information in latest years has caused a growing want for stable and green document garage and sharing answers [1]. Traditional centralized strategies, in which information is saved and controlled through a vital authority, have obstacles in phrases of information privateness, safety, and availability [2]. The centralized version is at risk of assaults, information breaches, and single point of failure. Furthermore, centralized strategies frequently depend upon third-celebration services, which could bring about extra fees, slower information switch rates, and lack of control over data [3].

To deal with those obstacles, decentralized technology which include blockchain and InterPlanetary File System (IPFS) have received reputation in latest years. Blockchain, initially evolved for virtual currencies which include Bitcoin, is an allotted ledger era that permits stable and obvious transactions without the want for vital intermediaries [4]. IPFS, on the opposite hand, is a peer-to-peer document machine that offers a decentralized and content-addressed garage version [5]. Together, blockchain and IPFS have the capacity to offer stable and green document garage and sharing answers with out the want for vital intermediaries or third-celebration services.

In this study, we advise a decentralized method for document garage and sharing the use of blockchain and IPFS. Our method leverages the immutability and transparency of blockchain era to make sure information integrity and safety, at the same time as documents are saved on IPFS to offer an allotted and content-addressed garage version. Access to documents is managed through clever contracts, which put in force predefined guidelines and permissions for sharing and editing documents. The technique proposed, ensures data availability by exploiting IPFS's content-addressing protocol. This technique ensures that documents can be viewed even if some nodes on the network become temporarily unavailable or go down. This decentralized strategy preserves the integrity and accessibility of the documents, resulting in a more resilient and dependable data retrieval solution.

The proposed method has numerous benefits over conventional centralized strategies. First, it presents stronger safety and privateness through leveraging blockchain's tamper-evidence and obvious nature [7]. Second, it removes the want for vital intermediaries, decreasing fees and growing information switch rates [9]. Finally, it presents information availability through leveraging IPFS's content-addressing scheme, making sure that documents may be accessed even though a few nodes within the community move offline [10].

To display the feasibility and effectiveness of our method, we carried out an evidence-of-idea prototype and evaluated its overall performance in phrases of information safety, scalability, and availability. Our effects display that the proposed method is scalable and might take care of a big variety of document requests with low latency and excessive throughput. We additionally performed a safety evaluation of our method and display that it's far proof against not unusualplace assaults which include information tampering, double-spending, and denial-of-service.

BACKGROUND

High prices, single points of failure, and susceptibility to data manipulation are problems with traditional centralized storage systems. By utilizing content-based addressing and distributed storage, decentralized solutions such as the InterPlanetary File System (IPFS) improve data availability, integrity, and cost effectiveness. By offering transparent permission management through smart contracts and unchangeable access restriction, blockchain technology enhances IPFS. Although earlier research has emphasized the advantages of integrating blockchain with IPFS for safe data exchange, including enhanced fault tolerance, speed of retrieval, and cryptographic integrity, scalability and effective access control continue to be major obstacles. By establishing a smart contract-based access control mechanism, this research expands on previous work and makes file sharing [11] safe, effective, and policy-driven.

A. Access Control

Access control is an important aspect of blockchain technology that ensures that only authorized users have access to and change data stored on the network. Blockchain access control is carried out using smart contracts to implement predefined access rules and policies. These smart contracts act as self-executing programs that automatically implement access control policies without the need for a central authority. Blockchain-enabled decentralized access controls have many advantages, such as transparency, adaptability, and tamper resistance. Access control rules are defined as intelligent contracts and cannot be modified without the consensus of network participants. This ensures that the access control policy is irrevocable and resists manipulation or unauthorized modifications. Several blockchain-based access control mechanisms have been proposed and implemented. For example, the Filecoin network uses smart contracts to define access control policies that ensure that only authorized users can access and modify stored data [12]. Similarly, the Store network uses a List of Access Controls(ACLs) to implement access control policies [13]. The blockchain's access control is also used in permissioned networks where network participants are known and trusted. Authorized blockchain networks, such as HyperledgerFabric, define access control policies based on role-based access control(RBAC). Access control is an essential aspect of blockchain technology for network security and integrity. Blockchain access control mechanisms have advantages compared to conventional access control mechanisms, such as transparency, invariability, and resistance to manipulation.

B. Blockchain and Smart Contracts

Blockchain and clever contracts are critical additives of allotted ledger generation which have revolutionized the manner we consider virtual transactions. Blockchain generation affords a decentralized, tamper-evidence, and obvious ledger of transactions, at the same time as clever contracts allow automatic execution of predefined guidelines and rules. A clever agreement is a self-executing software that robotically executes the phrases of a settlement among or greater parties. Smart contracts are coded in a programming language this is completed at the blockchain, making sure that the phrases of the settlement are robotically enforced with out the want for a third-birthday celebration intermediary. Smart contracts may be used to automate a huge variety of transactions, from easy fee transfers to complicated economic derivatives. One of the important thing advantages of clever contracts is their cappotential to automate the execution of complicated economic transactions. For example, clever contracts may be used to create decentralized self sufficient organizations (DAOs) that robotically execute predefined guidelines and rules with out the want for human intervention. DAOs may be used to create decentralized marketplaces, prediction markets, and different complicated economic structures. Blockchain generation affords a stable and tamper-evidence ledger of transactions this is maintained with the aid of using a decentralized community of participants. Blockchain

generation is frequently used to create cryptocurrencies which includes Bitcoin and Ethereum, which allow stable and nameless virtual transactions. However, blockchain generation has many different ability programs past cryptocurrencies, which includes deliver chain management, vote casting structures, and virtual identification management.

Blockchain generation and clever contracts are frequently used collectively to create decentralized programs (dApps) that automate complicated approaches and transactions. dApps are decentralized due to the fact they run on a blockchain community, which guarantees that they're obvious, stable, and immune to tampering. dApps may be used to create decentralized marketplaces, prediction markets, and different complicated economic structures which are greater green and stable than conventional centralized structures. One of the demanding situations of blockchain and clever agreement generation is scalability. Currently, maximum blockchain networks can most effective cope with a restrained quantity of transactions consistent with second, which limits their cappotential to scale to assist large-scale programs. However, there are ongoing efforts to enhance the scalability of blockchain networks, which includes the implementation of sharding and off-chain solutions. In conclusion, blockchain and clever contracts are critical additives of allotted ledger generation which have the ability to revolutionize the manner we consider virtual transactions. Smart contracts allow automatic execution of predefined guidelines and rules, at the same time as blockchain generation affords a decentralized, tamper-evidence, and obvious ledger of transactions. Together, blockchain and clever contracts may be used to create decentralized programs which are greater green, stable, and obvious than conventional centralized structures [13] [14].

C. IPFS

IPFS is a decentralized and distributed file storage and sharing system [5][6]. Instead of relying on a central server to store and serve files, it stores files on a distributed network of nodes. This makes it more secure and more resistant to censorship. IPFS uses the Content Addressing System to locate and retrieve files. This means that anyone with a copy of the files can see them, regardless of where they are on the network [5][6]. In addition, IPFS reduces file redundancy, making it more efficient and scalable than mainframe systems. IPFS outperforms traditional file storage systems in terms of speed and efficiency. Because files are stored on a distributed network, they can be retrieved more quickly and efficiently than in centralized systems. Also, because IPFS uses a peer-to-peer network, it can reduce the load on individual nodes, making them more scalable than centralized systems [5][6]. In summary, IPFS is a decentralized and distributed file storage and sharing system that offers several advantages over traditional centralized file storage systems. IPFS uses a content addressing system to locate and retrieve files, which reduces duplication and increases efficiency. In addition, IPFS is more secure and resistant to censorship than centralized systems, making it an attractive choice for those who value privacy and security.

D. Transactional Workflow in Blockchain

In a blockchain network, a transaction is a report of an occasion that has occurred, which include the switch of cryptocurrency or the execution of a clever contract. The transaction workflow in blockchain networks includes numerous steps, every of which performs a crucial position in making sure the safety and reliability of the transaction. The first step withinside the transaction workflow is the introduction of a transaction through a user. This transaction consists of info which include the sender`s public address, the recipient's public address, and the quantity of cryptocurrency being transferred. Once the transaction has been created, it's far broadcast to the community. The 2nd step is transaction validation. In order for a transaction to be taken into consideration legitimate, it need to meet sure criteria. For example, the sender need to have enough price range to cowl the transaction, and the transaction need to be signed with the sender's non-public key. Validation is normally carried out through nodes at the community referred to as miners or validators, who affirm the transaction's validity and upload it to a block. The 0.33 step is block introduction. Once a miner or validator has showed the transaction's validity, it's far introduced to a block at the side of different confirmed transactions. The miner or validator then provides a header to the block, which incorporates a cryptographic hash of the preceding block, growing a sequence of blocks which can be connected together, as a result the call blockchain. The fourth step is block validation. Once a block has been created, it need to be confirmed through different nodes at the community. Nodes validate the block through checking that its header consists of a legitimate cryptographic hash of the preceding block, and that the block's transactions are legitimate and regular with the blockchain's regulations and protocols. Finally, the block is introduced to the blockchain, and the transaction is complete. The transaction is now recorded at the blockchain, and its info may be considered through every person with get right of entry to to the community. Overall, the transaction workflow in blockchain

networks is a complicated technique that includes more than one steps and more than one nodes. However, this technique is crucial for making sure the safety and reliability of transactions at the blockchain.

E. Sharding

Our project here is utilizing sharding that implements a partitioning scheme to store data in a redundant and decentralized way. This is achieved using the interplanetary file system, a library that allows you to create multiple IPFS nodes that can store blocks of data between them. For those who may not be familiar with the term, sharding is a technique for storing and retrieving large files by breaking them into smaller pieces and distributing them across multiple storage nodes. This method is especially useful when dealing with files that are too large to fit on a single node. In this code, a string of data is retrieved and split into chunks, each of which consists of multiple chunks. These chunks are then stored on different nodes to provide redundancy and avoid any possibility of data loss. To facilitate communication between these nodes, IPFS pubsub is used. This allows nodes to publish and subscribe to messages on a specific topic. In this case, the icon shares a pub topic called "hash". When a node receives a message about it, it tries to download the corresponding fragment and reassemble it. After downloading and packaging all the scores, the code sends the compiled data string to the controller. This amazing piece of code demonstrates how sharding can be used to store and retrieve large files in a decentralized and redundant way using the power of IPFS.

PROPOSED SYSTEM

Our proposal for a secure file sharing system is based on the utilization of permission-less blockchain and IPFS, which is a decentralized method of recording transactions. While permission-less blockchain allows any user to participate in the network, it presents a challenge when it comes to validating users since there is no trusted central party. This can result in permission issues in the file sharing mechanism. To address this problem, we have designed a distributed access control and group key management system that utilizes the IPFS proxy.

The motivation for our proposed system is rooted in the fact that the nodes in the blockchain network have memory limitations, and only transaction records can be stored on the blockchain rather than complete files. This is where IPFS comes in as it is capable of storing relatively large data. However, it is important to note that IPFS and blockchain do not take into consideration computation overheads and security risks. As a result, our proposed system seeks to improve on these issues by providing a secure file sharing scheme that manages access control policies through the use of the IPFS proxy.

A. Challenges

Developing a blockchain-primarily based totally record garage and sharing device the usage of IPFS generation is a complicated assignment that calls for cautious attention of numerous important demanding situations. One of the maximum extensive demanding situations is scalability. IPFS has boundaries at the quantity of nodes which could take part withinside the community, that could preclude the community`s capacity to shop huge quantities of records. Therefore, it's far vital to make certain that the device is scalable and might accommodate a huge quantity of contributors and records. Security is every other primary difficulty whilst constructing a blockchain-primarily based totally record garage and sharing device. While blockchain generation gives an excessive degree of security, IPFS does now no longer provide the identical degree of protection. As a result, it's far crucial to make certain that records saved on IPFS is encrypted and guarded from unauthorized access. Additionally, keeping the safety of the blockchain community, along with stopping 51% attacks, is important to keeping the integrity of the device. Interoperability is likewise an extensive assignment whilst constructing a blockchain-primarily based totally record garage and sharing device. The device need to make certain that records may be shared throughout specific blockchain networks and IPFS nodes. This calls for the improvement of a wellknown protocol for records garage and sharing that may be utilized by all networks. Decentralization is every other important assignment that the device need to overcome. The device need to make certain that it's far completely decentralized, that means that no significant authority controls the community. This calls for the improvement of a consensus set of rules that guarantees the community stays steady and the records saved on it's far tamper-proof. The excessive strength intake related to blockchain generation is every other assignment that the device need to address. The system of mining blocks in a blockchain community calls for a extensive quantity of computational power, which consumes a whole lot of strength. Therefore, it's far crucial to make certain that the device is strength-efficient, and the mining system does now no longer damage the environment. Finally, the adoption of the device is likewise an extensive assignment. Blockchain-primarily based totally record garage and sharing is an exceptionally new concept, and plenty of humans aren't acquainted with the generation.

Therefore, teaching humans approximately the blessings of the device and the way it works is vital to its success. In summary, constructing a blockchain-primarily based totally record garage and sharing device the usage of IPFS generation poses numerous important demanding situations, consisting of scalability, security, interoperability, decentralization, strength intake, and adoption. Overcoming those demanding situations calls for the improvement of progressive answers and the collaboration of specialists in blockchain, IPFS, and cybersecurity.

B. System Model

The solution we propose here is to create a distributed data storage system that will store data in a peer-to-peer network so that there is no central body and the ability to use and change the data market. The data will be divided into several pieces, encrypted using different crypto algorithms, and stored on different nodes. No, each node will know the data and whose data it is storing. Even if an attacker breaks the hole and extracts the data, they will only get access to part of the encrypted data. This makes it difficult to capture the complete data of each individual that has been compromised. It is more secure than the cloud [8]. For data storage services, the network provider's storage space will receive a fee and the customer will pay minimal to no fees for this service depending on network stress. In addition, the customer and the sender of the letter will be linked to a "smart contract" stored in the Blockchain that will be a proof of trust layer for data access and storage. In this way, the network will be supported by a reward and compensation system. The data blocks and trust of the database are managed using blockchain.

The flow for this would be quite simple. The application only needs a file from the user as user input and the system will upload that file with a set of the private key that is provided by the user.

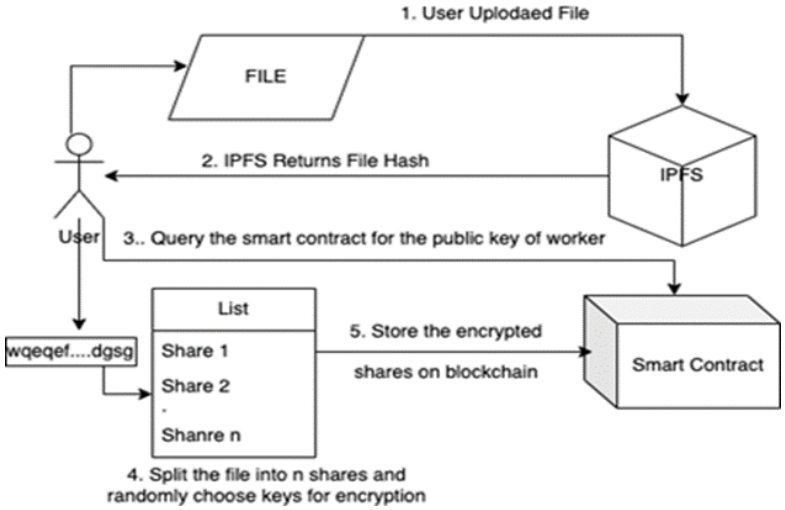

Fig 1. Proposed File Sharing System

The blockchain-based IPFS file sharing and storage system can be designed as a three-way system consisting of owners, users, and the IPFS network. Owners are responsible for downloading and storing files on the IPFS network, while users retrieve files from the network. The IPFS network acts as a decentralized storage infrastructure, making it easy to store and retrieve files. The owner initiates the file storage process by uploading the file to the IPFS network. The file is split into small blocks and a unique hash is generated for each block. The hash is stored on the blockchain, ensuring the integrity and immutability of the file. The owner can access the file by providing an IPFS network hash. The owner is also responsible for managing file access control, defining who can access them and what level of access they have. Users retrieve files from an IPFS network by asking the owner to hash the file. Users can then access the file by providing the hash to the IPFS network. The IPFS network locates the file elements and reassembles them for the user. Users can access files without relying on central servers or storage facilities, ensuring that data is available and accessible. The IPFS network acts as the backbone of the system, facilitating file storage and retrieval. The IPFS network is a distributed system that stores data on nodes around the world. When a file is uploaded to an IPFS network, it is split into smaller pieces and distributed across multiple nodes. This ensures that data is always available even if some nodes are offline. This system model ensures data security through a decentralized method of file storage and retrieval. Using the blockchain ensures file integrity and immutability, while the IPFS network ensures availability and accessibility. The system model also provides access control, which allows owners to decide who can access files and what level of access they have. In summary, the system model of the blockchain-based IPFS file

sharing and storage system can be designed as a three-way system consisting of owners, users, and the IPFS network. Owners are responsible for downloading and storing files on the IPFS network, while users retrieve files from the network. The IPFS network acts as a decentralized storage infrastructure, making it easy to store and retrieve files. This system model ensures data security through a decentralized approach to file storage and retrieval, and access control mechanisms allow owners to decide who can access files and their level of access.

C. Workflow

The workflow of the blockchain-based file sharing and storage system provided by IPFS can be divided into several phases. The first stage is the file transfer stage, where the owner uploads the file to the IPFS network using the IPFS node. Downloaded files are encrypted and then broken into smaller pieces, which are then distributed over the IPFS network. File segments are replicated across multiple IPFS nodes, ensuring that files are always available and accessible, even if one node fails or goes offline.

The second stage is the user authentication stage, where users who want to access shared files on the blockchain must be authenticated. Once approved, the user can access and download the file from the IPFS network. The blockchain verifies user identities and ensures that only authorized users can access shared files.

The third stage is the file transfer stage, where users download shared files from the IPFS network. During the download process, IPFS nodes retrieve file fragments from the network and reassemble them into the original file. The uploaded file is then decrypted with the owner's private key, so that only authorized users can access the original file. The proposed system model consists of three main parts: owners, users, and IPFS network. Owners upload files to the IPFS network and users authenticate to the blockchain to access shared files. The IPFS network is responsible for storing and replicating file segments across multiple nodes, ensuring that files are accessible and accessible at all times.

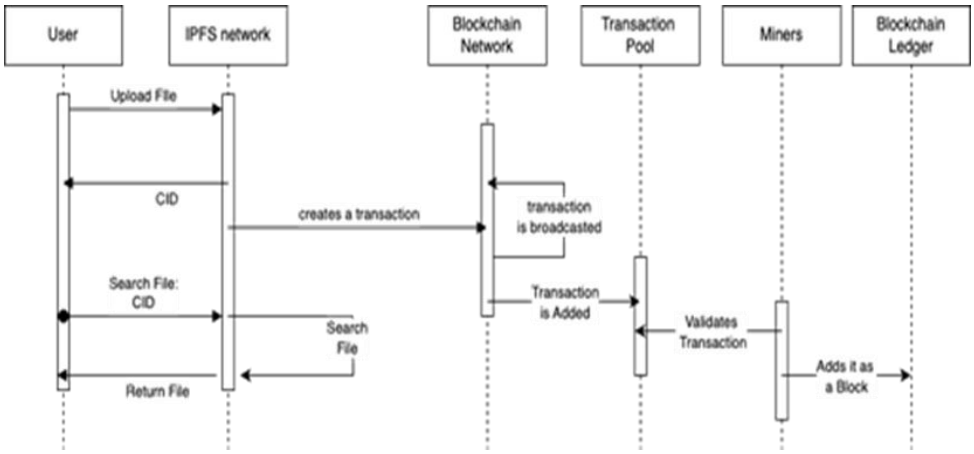

Fig 2. Sequence Diagram

The demonstration sequence diagram of the proposed system model as illustrated in Fig 2, the file sharing and storage workflows. Sequence diagram showing the interaction of the owner, user, IPFS, and blockchain components during file upload, user authentication, and file transfer. Overall, the proposed system model and workflow for blockchain-based file storage and sharing with IPFS demonstrates a secure and decentralized approach to data storage and sharing. The use of encryption, authentication and transcription ensures that files are protected against unauthorized access and are always easily accessible to authorized users.

The Blockchain and IPFS-based secure file storage and sharing mechanism allows for decentralized, private, and tamper-resistant data management. The process begins with user authentication, in which each user generates a public-private key pair and stores the public key on the blockchain while keeping the private key secure. Files are encrypted, separated into chunks, and uploaded to IPFS, with each piece assigned a unique hash for integrity verification. Content Identifiers (CIDs) and access control rules are maintained on the blockchain and managed via smart contracts. When a file is shared, the encryption key is secured using the recipient's public key, and access permissions are enforced through smart contracts. The recipient obtains CIDs, retrieves encrypted chunks from IPFS, decrypts the file, and verifies its integrity using hash values. Blockchain consensus mechanisms like PoS or PoA safeguard against unauthorized

modifications. Storage providers earn rewards for hosting data, while users pay minimal fees, with smart contracts automating transactions. The steps are given in below algorithm. This approach ensures a secure, efficient, and decentralized system for file storage and sharing.

Algorithm for Secure File Storage and Sharing

Step 1: User Registration and Key Generation

1. User registers on the system
2. Generate (PublicKey, PrivateKey) using ECDSA
3. Store PublicKey on blockchain
4. Keep PrivateKey secure with user
5. Define access control policies for user files

Step 2: File Encryption and Segmentation

1. User selects FILE to upload
2. Split FILE into multiple CHUNKS
3. FOR each CHUNK in FILE:
   a. Encrypt CHUNK using AES-256 → ENCRYPTED_CHUNK
   b. Compute HASH = SHA-256 (ENCRYPTED_CHUNK)
   c. Store HASH in metadata
4. Encrypt AES encryption key with user's PublicKey

Step 3: Store Encrypted Data on IPFS

1. Upload ENCRYPTED_CHUNKS to IPFS
2. Get unique Content Identifiers (CIDs) for each CHUNK
3. Store (CIDs, Access Policies, Encrypted Key) on Blockchain via Smart Contract

Step 4: File Sharing and Access Control

1. IF User wants to share FILE with Recipient:
   a. Encrypt AES Key with Recipient's PublicKey → ENCRYPTED_ACCESS_KEY
   b. Update Smart Contract with Recipient's access rights
2. Recipient requests access from Smart Contract
3. Smart Contract verifies access permissions
4. IF access granted:
   a. Retrieve ENCRYPTED_ACCESS_KEY from Blockchain
   b. Decrypt ENCRYPTED_ACCESS_KEY using Recipient's PrivateKey → AES_KEY

Step 5: File Retrieval and Verification

1. Retrieve CIDs from Blockchain
2. Fetch ENCRYPTED_CHUNKS from IPFS
3. FOR each CHUNK:
   a. Decrypt using AES_KEY → DECRYPTED_CHUNK
   b. Compute HASH_NEW = SHA-256(DECRYPTED_CHUNK)
   c. IF HASH_NEW == HASH (stored in metadata)
      - File integrity is verified
   ELSE
      - Data corruption detected
4. Reassemble FILE from DECRYPTED_CHUNKS

Step 6: Security and Consensus

1. Blockchain consensus (PoS/PoA) ensures transaction integrity

2. Smart Contract enforces access control and permissions
3. Implement 51% attack protection mechanisms

Step 7: Incentives and Payments
1. Storage providers receive rewards for hosting encrypted file chunks
2. Users pay minimal fees for storage based on network demand
3. Smart Contract automates payments and rewards

D. Access Control in IPFS

IPFS is a distributed peer-to-peer network that allows content to be stored and shared without relying on a central authority. Therefore, it is important to have appropriate access control mechanisms in place to ensure the security and privacy of shared data. In this context, access control refers to the process of managing and enforcing permissions and restricting who can access, edit, or delete content on an IPFS network. One way to control access to IPFS is to use access control lists (ACLs). ACLs are a technology widely used in computer security that allows resource owners to determine who can access that resource and what they can do with it. In IPFS, an ACL can be defined for a specific file or directory, specifying the addresses of users or groups authorized to access it. Another way to control access to IPFS is to use encryption. This includes encrypting shared data with keys that only authorized users can access. Encryption ensures that even if unauthorized users access the data, they cannot read or modify it without the key. One of the challenges of IPFS access control is the decentralized nature of the network. Unlike traditional client-server architectures, there is no central authority to manage access control policies. Instead, each user is responsible for managing their own shared data access control policies.

To address this challenge, IPFS introduces a concept called the "IPNS Namespace". IPNS namespaces allow users to assign a name to their content that translates to the content website. With IPNS namespaces, users can manage access control policies for their content by assigning permissions to specific names instead of specific IPFS addresses. Another challenge in controlling access to IPFS is the possibility of unauthorized modifications of shared content. To address this, IPFS includes a feature called "Content Handling", which ensures that any changes to the content result in a new hash. This means that any unauthorized modification of the content will result in a different hash, and users can detect such modifications by comparing the hashes. In summary, access control is an important aspect of ensuring the security and confidentiality of shared data in an IPFS network. Access control mechanisms such as access control lists and cryptography can help manage and enforce permissions and restrictions on who can access data. However, the decentralized nature of the network presents significant challenges in managing access control policies. IPFS features such as IPNS namespaces and content handling help solve some of these challenges and provide a secure and decentralized way to control access to IPFS.

E. Group Management and Security

By implementing IPFS access controls and storing files on the blockchain, various security features can be leveraged. These features are designed to ensure data integrity and privacy and work together to create a robust and secure file management and access platform. The use of encryption keys is one of the main security features. These keys are used to protect files stored in IPFS and each group has its own unique encryption key. This key is encrypted with the user's public key to ensure that only authorized users can access files in their private groups. Another important security feature is the use of blockchain technology. Each file is stored as a block in the blockchain and changes made to the file will be saved as a new block. This creates an immutable record of the file's history, ensuring data integrity and eliminating the possibility of unauthorized manipulation or modification. Access control is also an essential security component. Users can only access files that are allowed by the groups they belong to. Each user has a unique public key that is used to encrypt and decrypt the group's encryption key, ensuring that only authorized users can access files in their own group. In addition, blockchain technology provides a secure and transparent platform for user permission management and access control. Automatic access control can be implemented using smart contracts, ensuring that only authorized users can access files. User permissions and access control can be managed using a decentralized management model, eliminating the need for centralized authorization and improving system security. In summary, implementing IPFS access control and file storage on the blockchain provides multiple security features that ensure

data confidentiality, integrity, and availability. The use of encryption keys, access control and blockchain technology creates a secure and transparent platform for file management and access, which increases data security, eliminates the possibility of manipulation and ensures that only those authorized users can access the files. With these features, users can rest easy knowing their data is safe. For example, in a scenario where Alice, Bob, and Charlie are 3 users of this system and Alice and Bob belong to group 1, and Bob and Charlie belong to group 2, Bob can access files belonging to both groups since he is a member of both. However, Alice can only access files in group 1, and Carol can only access files in group 2.

RESULTS AND DISCUSSION

The explosive growth of digital data opens the way for secure and scalable file storage and sharing. Conventional centralized storage solutions face various issues such as high operational costs, single-point failures, and risks of data breaches or corruption. Such limitations motivate searching for alternatives that can be resilient and cost-effective instead. The InterPlanetary File System (IPFS) takes a centrally distributed storage mechanism since it houses data across many nodes as opposed to hosting a server of one kind only in one central server. This increases fault tolerance, retrieval speed, and bandwidth usage in the process. Cryptographic hashing mechanisms are now used to ensure data integrity by flagging when data undergoes alteration or corruption without prior notice.

The interoperability of blockchains allows for enhanced security and access control in decentralized storage systems. Smart contracts automate permission management, ensuring that files are accessed only by authorized users, while consensus mechanisms such as Proof-of-Stake (PoS) and Proof-of-Authority (PoA) prevent unauthorized modifications. This work investigates the hybrid use of IPFS and blockchain for secure file storage and sharing. A comparative analysis shows that this method holds advantages when it comes to retrieval speed and cost efficiency to verification of data integrity, and fault tolerance. This is scalable and secure in contrast to conventional storage mechanisms, further expanding their limitations.

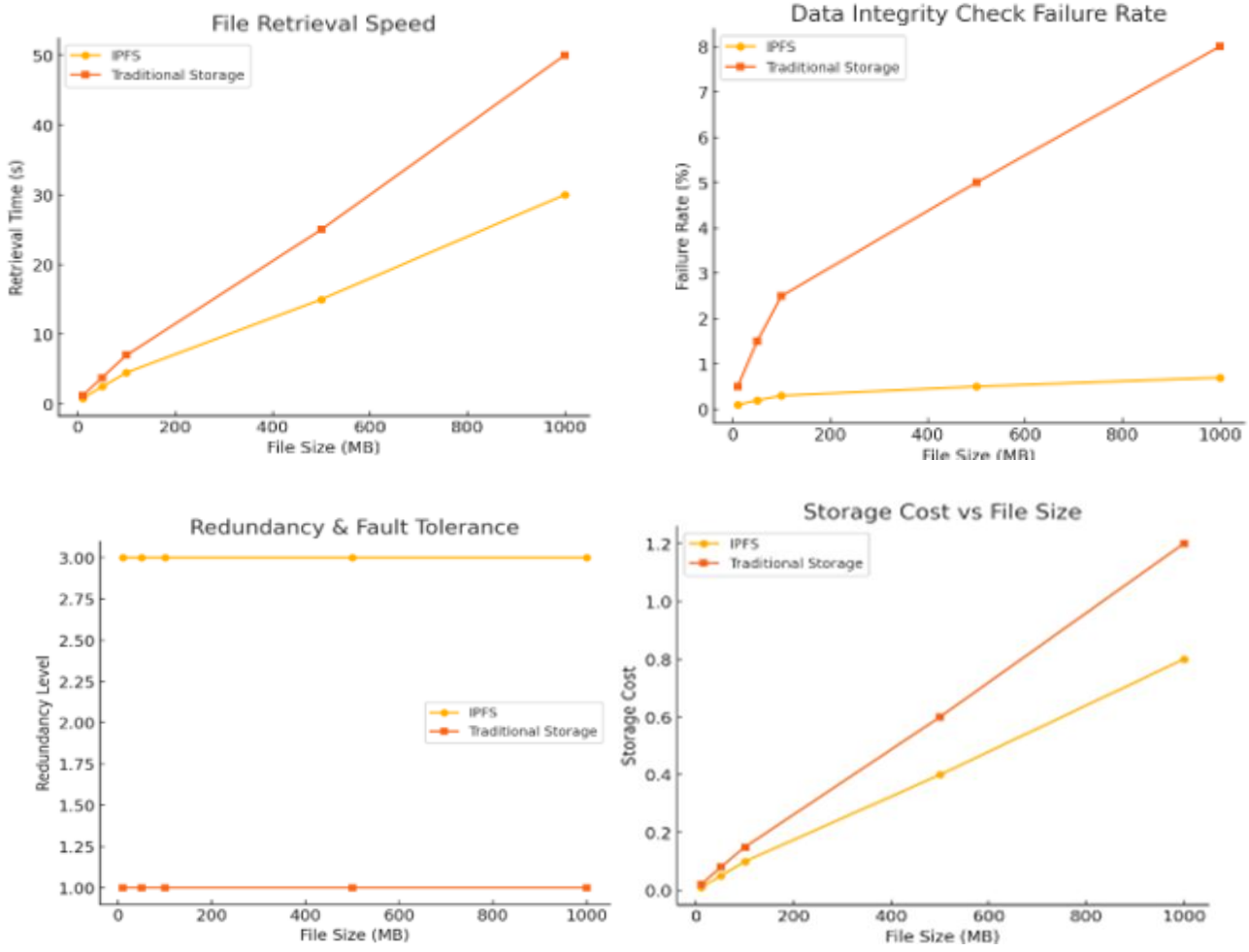

Fig. 3 Comparative study shows IPFS has advantages over the traditional centralized storage

The comparative study of the file storage solutions shows that IPFS has its advantages over the traditional centralized storage. In terms of speed of file retrieval, the performance of IPFS overtakes the traditional storage by grace of its distributed nature that allows a number of nodes to fetch data simultaneously, hence, decreasing retrieval time with increasing file sizes. Further analysis of storage costs shows that IPFS saves costs because it does not resort to centralized infrastructure and rather relies on a decentralized network; given how traditional storage has considerably high operational expenses asshown in above Fig.3.

On top of that, data integrity checks demonstrate that IPFS has shown less failure rates, thanks to cryptographic hashing (SHA-256), ensuring files remain unaltered and in proper condition and greatly reduce chances of corruption that usually plague centralized storage. IPFS has also made significant strides in improving redundancy and fault tolerance by storing files across multiple nodes to prevent data loss in case of server failure. Traditional storage is more prone to outages and loss of data as it relies on single-point systems. Thus, results show that IPFS, in combination with blockchain technology, provides a more secure, efficient, and cost-effective alternative to traditional file storage and sharing methods. These insights demonstrate IPFS as a superior alternative, offering improved security, efficiency, and cost savings for decentralized file storage.

CONCLUSION

By combining blockchain technology with the InterPlanetary File System (IPFS), this study presents a safe and decentralized method of file sharing. Our technology uses blockchain-based smart contracts and encryption approaches to improve data security, privacy, and access management. Our technology removes single points of failure and guarantees that sensitive data is protected without relying on a central authority, in contrast to conventional file-sharing techniques that rely on centralized storage. By using blockchain-enforced permissions and group-based encryption, the system guarantees safe access control. Groups can be created or joined by users, and smart contracts and cryptographic keys control access. Only authorized users can decrypt files thanks to key rotation, which facilitates easy access revocation.

With AES-256 encryption for data protection and SHA-256 hashing for integrity verification, this approach guarantees security. Secure retrieval and access control are automated using blockchain smart contracts. By using an incentive concept, our approach ensures data sustainability and availability while rewarding storage providers. We offer a safe, decentralized, and scalable solution for regulated data exchange by utilizing blockchain, IPFS, encryption, and smart contracts. Organizations with stringent confidentiality and integrity requirements will find this framework especially helpful. Future research will concentrate on improving performance, expanding scalability, and investigating uses in secure government communications, healthcare, and finance.

REFERENCES

[1] IDC, "Data Age 2025: The Evolution of Data to Life-Critical," IDC White Paper, 2017.
[2] D. Agrawal and A. Dubey, "A Comparative Analysis of Decentralized Storage Technologies," IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2019.
[3] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin.org, 2008.
[4] C. Cachin, R. Guerraoui, and L. Rodrigues, "Introduction to Reliable and Secure Distributed Programming," Springer International Publishing, 2011.
[5] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," arXiv preprint arXiv:1407.3561, 2014
[6] A. Mishra, S. Verma, Ankit, “Blockchain-Based File Storage using IPFS: A Secure and Transparent Approach”, May 2023, DOI:10.13140/RG.2.2.22075.18722.
[7] C. Wang, Q. Wu, J. Xu, and K. Ren, "Privacy-Preserving Decentralized Storage Systems," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 4, pp. 393-405, 2017.
[8] P. Sharma, S. Namasudra, and P. LORENZ, “Blockchain-based Cloud Storage System with Enhanced Optimization and Integrity Preservation”, in 2023 IEEE International Conference on Communications (ICC): SAC Cloud Computing, Networking and Storage Track, DOI: 10.1109/ICC45041.2023.10279598, May 2023.
[9] S. Tai, S. Ma, Y. Zhang, and L. Hu, "A Blockchain-Based Decentralized Storage System," IEEE International Conference on Networking, Architecture, and Storage (NAS), 2018.
[10] D. Meijer and J. Garcia-Alfaro, "A Survey on Decentralized Data Storage Systems," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 674-695, 2020.

[11] Wanzong Peng, Tongliang Lu, Wenju Peng & ZhongpanWang, “An efcient blockchain-based framework for fle sharing”, https://doi.org/10.1038/s41598-024-69011-4, Apr. 2024.
[12] J. Benet, "Filecoin: A Decentralized Storage Network," Filecoin White Paper, 2017.
[13] S. Wilkinson, "Storj: A Peer-to-Peer Cloud Storage Network," Storj White Paper, 2014.
[14] H. ZANG, HO KIM, and JONGWON KIM, “Blockchain-Based Decentralized Storage Design for Data Confidence Over Cloud-Native Edge Infrastructure”, Doi: 10.1109/ACCESS.2024.3383010, Vol.12, pp. 50083-50099, Apr. 2024.
[15] A. Antonopoulos, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies," O'Reilly Media, 2014.
[16] Dong, Changyu & Russello, Giovanni & Dulay, Naranker. (2011). Shared and searchable encrypted data for untrusted servers. Journal of Computer Security. 19. 367-397. 10.3233/JCS-2010-0415.
[17] Shafagh, Hossein & Burkhalter, Lukas & Hithnawi, Anwar & Duquennoy, Simon. (2017). Towards Blockchain-based Auditable Storage and Sharing of IoT Data. 45-50. 10.1145/3140649.3140656.
[18] Nguyen, Linh & Nguyen, Lam & Hoang, Thong & Bandara, Dilum & Wang, Qin & Lu, Qinghua & Xu, Xiwei & Zhu, Liming & Popovski, Petar & Chen, Shiping. (2023). Blockchain-Empowered Trustworthy Data Sharing: Fundamentals, Applications, and Challenges. 10.48550/arXiv.2303.06546.