A Trustless Cloud Storage Framework Integrating IPFS and Solidity Smart Contracts

Aman Chaudhary
Department of Computer Science and Engineering
Meerut Institute of Engineering and Technology, Meerut
Email: aman.chaudhary.cse.2022@miet.ac.in

Aryan Siwach
Department of Computer Science and Engineering
Meerut Institute of Engineering and Technology, Meerut
Email: aryan.siwach.cse.2022@miet.ac.in

Bhavy Singhal
Department of Computer Science and Engineering
Meerut Institute of Engineering and Technology, Meerut
Email: bhavy.singhal.cse.2022@miet.ac.in

Priyanka Dhanraj
Department of Computer Science and Engineering
Meerut Institute of Engineering and Technology, Meerut
Email: priyanka.dhanraj@miet.ac.in

***Abstract*—The rapid increase in digital data has led to heavy reliance on centralized cloud computing. Consequently, users are exposed to critical vulnerabilities, including unauthorized access, privacy invasion, and single points of failure. This study proposes a cloud storage system that is trustless to address these challenges that have persisted. The underlying methodology utilizes distributed data hosting based on the InterPlanetary File System (IPFS) and decentralized access control through Solidity smart contracts. Under this architecture, file metadata is stored safely on an unalterable blockchain registry, and the media files are stored off-chain. These contracts are automatically run by granular access controls like specific public and private visibility modes. At any point, no outside intervention of a third party is needed. The system was checked during the testing time in terms of a functional accuracy in regards to a secure storage, verifiable retrieval, and instant revocation of permissions. According to the key results, the elimination of intermediary control, prevention of unauthorized access to data attempts, and high data availability are achieved. In conclusion, this shows that a combination of programmable smart contracts and peer-to-peer storage will provide a potentially scalable and secure alternative to the traditional cloud architecture. This leads to a considerable improvement in user data sovereignty and systemic resilience as a whole.**

***Index Terms*—Ethereum, Solidity, IPFS, Smart Contracts, Decentralized Storage**

I. Introduction

The recent years have experienced an extreme increase in the volume of digital data. This has led to the creation of increased dependence on centralized cloud systems to run information processing and data storage. Although services such as Google Drive and Dropbox are widely used, they are built on the basis of fundamentally centralized architectural designs. In such structures, these third-party organizations retain great control over the information they get as provided by the users. This centralization provokes several critical issues such as massive data breaches, vulnerabilities to unauthorized access, thorough censorship, and single points of failure, among others [1], [7]. As such, the background of the issue is inherent risks of delegating sensitive digital resources to centralized power, where the sovereignty of the user data is technically lost.

In order to comprehend the solution proposed, it is necessary to define certain terms concerning the decentralized technologies. Decentralized storage is described as a network in which data is stored in a number of autonomous network nodes instead of being stored on one trusted server. The blockchain technology is based on the principle of immutability and transparency and is used to offer a secure means of storing ownership rights and access control rights with no central authority involved in any of these functions. Moreover, InterPlanetary File System (IPFS) is a peer-to-peer (P2P) distributed file protocol. IPFS uses content-based addressing as opposed to traditional location-based addressing. A Content Identifier (CID) is a special cryptographic hash used to request files, thereby making the stored data resistant to manipulation and server failures highly resilient to files being deleted and restored again [2], [4]. Last but not the least the use of smart contracts (self-executing programmable rules deployed directly on the blockchain) is leveraged to automatically administer access control policies to users [10], [11].

The main objective of this study work is to design and test a trustless cloud storage model. A secure, transparent, and tamper-resistant alternative to regular cloud services is proposed by combining IPFS-based distributed data hosting with blockchain-based access control; this allows achieving high levels of security, transparency, and resistance to tampering and alteration by unauthorized parties, among other benefits, [6], [14]. This architecture allows giving the absolute control back to the user with regard to personal data. The dangers of having a few major service providers are greatly mitigated and practical evidence is given to prove that decentralized models can be highly scalable and practical by effectively replacing their traditional data storage model.

II. Background and Theoretical Framework

Decentralized clouds storage systems are designed with the help of several major technologies such as blockchain, distributed hash-based storage, and smart contracts. The following section will present very briefly the key theoretical concepts according to which the proposed solution will be designed.

A. Blockchain and Distributed Ledger Technology

Blockchain is a type of distributed ledger technology where transactions are grouped together into blocks, and a cryptographic hash is added to relate them with one another. Each member possesses an identical copy of the ledger and there are consensus protocols that ensure that all the honest nodes are aligned to achieve a common state [7]. As an append-only and immutable storage, blockchain provides a stable form of ownership, access control, and history of the system in a form that is hard to alter and re-write. These attributes enable blockchain to be applied to cryptocurrencies and requirements that need audit trials that can be verified and transparent governance [9], [15].

B. InterPlanetary File System (IPFS)

IPFS is a P2P distributed file system that employs content addressing rather than traditional location addressing. Users do not request a file on a particular server but rather request content using its hash, known as Content Identifier (CID). This would allow any node with a copy of the file to serve it to increase redundancy and also to resist single points of failure [2], [10]. IPFS can be combined with blockchain to make separation of concerns, the large files are off-chained in distributed network and lightweight metadata (e.g. CIDs and ownership information) are on-chained on blockchain [4], [11]. This hybrid structure is required to make sure that the blockchain is not flooded.

C. Smart Contracts and Access Control

Smart contracts are programs that are automatically run in a blockchain and act according to set rules. In terms of storage, they are used to encode access policies, document file ownership and deterministically apply changes in permission changes on the files [5], [6]. Unlike traditional access control lists that are stored in centralized servers, the logic of smart contracts is publicly verifiable and can be executed in the same fashion by everyone. This allows it to have fine-grained access control whereby a user may grant or revoke permission and each action is documented in an immutable fashion. These are the properties that are significant in the development of trustworthy decentralized storage platforms [12], [13].

III. Related Work

A considerable number of studies have been dedicated to enhancing the cloud storage security and reduction of dependence on centralized services providers. Traditional clouds are founded on the trust model where users must relinquish their data to third-party organizations to store their data and administer it and it is vulnerable to unauthorized access and data leakage and single point of failure is not excluded of all [1]. It is on these flaws that the scholarly community has aimed to explore the notion of decentralized architectures that emphasize on transparency, integrity, and data sovereignty. The literature contains several research works that propose blockchain-based solutions to improve the management of data access and eliminate intermediary organizations [16], [17].

A case of how the distributed storage can be used to increase the data confidentiality and reliability is an integrated blockchain and IPFS system to operate the source code repositories offered by Haque et al. [2]. Similarly, Bandanadam et al. proposed a decentralized auditing system that is built on a dynamically changing cryptography to create data integrity in a cloud-based system and recommended that blockchain could deliver tamper-resistant verification without requiring disclosure of the content origin in the source more generally called [3].

The use of smart contracts to implement secure access control schemes in a decentralized system has been discussed in literature by other researchers. A system proposed by Chintal et al. utilized Solidity-based contracts to control storage practices, prevent unauthorized changes, and increase the traceability of distributed networks [4]. In addition, Prabanand et al. demonstrated that smart contracts may be deployed to secure financial systems in private Ethereum networks, and that programmable blockchain logic has a greater potential in access governance [5].

It has also been pointed out that IPFS integration with blockchain technologies may be marked as one of the promising research directions. The study by Cong et al. and Peng et al. proved the decentralized file sharing and copyright protection systems, and they revealed that the IPFS-based systems had the ability to offer the data availability, maintain the content authenticity and the anti-tampering resistance of the data file-sharing system [10], [11]. In other applications by researchers, a paradigm of decentralized storage has been applied in domain-specific applications, including synchronizing electric vehicles and certifying halal processes, demonstrating the utility of IPFS and smart contracts beyond the context of cloud storage storage [12], [13].

Although the above solutions are valuable in the process of creating secure and decentralized storage solutions, most of them are either lacking in user-level permission, which is fine-grained, or they lack a practical mechanism of content display in real-time. Moreover, most of the proposed models are silent on usability issues and therefore not easy to users not in the technical field. The present study can be considered unique because it combines blockchain-based ownership tracing, IPFS-based data storage and easy-to-use access controls, such as a public/private visibility mode and selective permission control, to offer a decentralized model of cloud storage that has usability and data sovereignty capabilities to it [6], [14].

IV. Problem Statement

The current cloud storage implementation is centralized in the facility of third parties that store, handle and regulate any data, and that is why this analysis presents a decentralized model of cloud storage and enhanced usability and data sovereignty. These convenient and scalable services have some vulnerabilities such as single points of failure, unauthorized access to data, privacy invasion and inability of the user to control what is stored therein despite its convenience and scalability features, weaknesses which are susceptible to hacking attacks that can damage all user data, and force the affected organization to resort to legal measures against the perpetrator to recover its reputation [1], [7]. The users must implicitly trust that their data is going to be protected by the service provider but numerous data breaches, stolen credentials, unauthorized surveillance and other incidents indicate how susceptible such systems can be.

The lack of transparency in the traditional cloud systems further aggravates the issue since users cannot have a verifiable system to determine whether their information has been accessed, modified or copied by the provider without their consent or not [6]. Therefore, even the sensitive data that is stored in centrally-hosted servers can be abused internally, attacked, censored, and suffer jurisdiction limitations and constraints [9]. These issues demonstrate a serious weakness of the existing cloud technologies, in which the user cannot have autonomy and data confidentiality.

Given the rising volume of digital assets and the rising amount of concern over the privacy of information, there is a rising need to possess a storage architecture, which provides provable possession of information, is governed by transparent terms, and is pushed out against uncertified modifications. The most essential part of the problem that the present study seeks to address is the absence of safe and user-friendly cloud storage paradigm which would ensure full sovereignty of the data with no dependency on the centralized powers. To overcome the limitations of the traditional cloud system in the present paper, a decentralized cloud solution will be proposed with the use of blockchain smart contracts and IPFS that will allow users to store and share their digital files without handing over their control to a third party [2], [4], [14].

V. Objectives

This study is defined through the creation of a decentralized and secure cloud storage architecture as its key goal. By using this proposed structure, users are granted absolute ownership and control over digital content and history is obviated as the centralized service providers are eliminated. In order to reach this general objective, other smaller sub-objectives are established:

- **Implement a distributed data hosting mechanism using the InterPlanetary File System (IPFS) to guarantee continuous data availability and eliminate single points of failure.**
- **Smart contracts are to be implemented based on blockchain to automatically impose fixed, transparent, and without other access control policies have verifiable access controls and intervention.**
- **Granular user permissions, in particular, including dual ones, modes of public and private visibility, should be enabled to offer flexible access control.**
- **Traceability and privacy of data will be increased by making certain that each and every permission change is forever stored in a decentralized blockchain registry.**
- **There should be a very easy to reach graphical interface that should be designed such that hidden technical complexities are definitized, hence streamlining the operations for non-technical users.**

VI. Proposed System

The proposed decentralized cloud storage system is designed to have an architecture built in five different phases of operation. An overview of the entire workflow that involves the execution is shown in the following flow diagram. All the stages are fully outlined below:

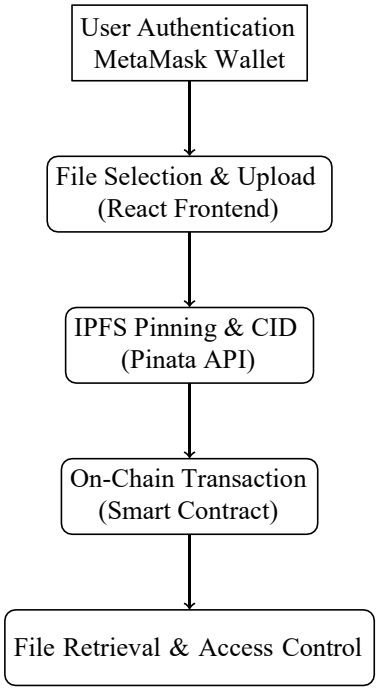

Fig. 1. System Flow Diagram

A. Phase 1: User Authentication and Interface Interaction

The system creates cryptographic identity verification first. A decentralized web3 wallet (e.g., MetaMask) is also used to authenticate a user instead of using username and password credentials. The user is linked to the React-based frontend interface and his or her personal Ethereum wallet address is retrieved. This address is then used as the primary identifier of all the future data ownership and access control operations.

B. Phase 2: File Upload and IPFS Pinning

When the user selects a media file, the information is handled by the client-side interface. The file is bundled and uploaded directly into InterPlanetary File System (IPFS) network using pinning service (Pinata API). With this distributed protocol the file is fragmented, hashed with cryptography and a unique Content Identifier (CID) is created. Accordingly, real media information has a safe off-chain storage.

C. Phase 3: Smart Contract Interaction and Blockchain Logging

After the CID is able to be retrieved over the IPFS network, a blockchain operation is started. The Ethereum network invokes the Solidity smart contract. The CID together with the wallet address of the user is safely mapped and it is imprinted permanently on the blockchain register. Through the implementation of this action, irrefutable ownership is created without being limited to storing large files on the blockchain.

D. Phase 4: Access Control and Permission Management

The smart contract is autonomously controlled by granular access control logic. In case an image is labeled as personal, it has to be specifically allowed by the proprietor. The owner can provide a targeted wallet address to enable access using the frontend interface. This step will cause the allow() operation in the contract, which will update the permission mapping that is decentralized. Access, on the contrary, can be revoked immediately through the disallow() method that will guarantee complete data sovereignty to the user.

E. Phase 5: File Retrieval and Display

The cryptographic permissions of the requester are checked by the smart contract when an image retrieval request is provided. In case authorization is authenticated, the stored array of CID is sent back to the front end. Lastly, the CIDs are actively optimized by an IPFS gateway, and the pictures are safe-rendered in the display of the user. Without authorization then a transaction is simply reverted and file access is denied.

VII. System Features and Use Case Scenario

The provided system will be not only technologically created as a prototype, but it is also practical. This section identifies the most significant features of it and gives a common application example.

A. Key System Features

- **Public and Private Visibility Modes:** Every file uploaded can be set to be publicly available or available to particular users. This dual mode architecture supports open sharing and confidential storage without modifying the underlying architecture.
- **Dropdown-Based Access Management:** The system does not require users to communicate with smart contracts directly, rather it offers a dropdown-based interface to authorize or deny access to selected blockchain addresses. This is simple and the barrier to entry is minimized by the non-technical users.
- **On-Chain Ownership Tracking:** File ownership is written on the blockchain, so there is always a verifiable source of truth of who uploaded a specific file, as well as who in turn is permitted to handle the permissions of the file.
- **Auditable Access History:** Permission changes and access operations are carried out through smart contracts, and thus are on-chain. This generates a record of interaction history that is auditable and may be reviewed in the event of dispute or regulatory demand.

B. Representative Use Case Scenario

Consider the case of a small academic research group that ought to share the image and findings of the experiment with the group members. Under normal cloud storage arrangement, the staff is expected to have one focal point, extensive access to folders and leave the service provider to take care of their data. The de-centralized storage system proposed has the principal researcher uploading the pictures to IPFS using the user interface and marking the pictures as confidential. In turn, each member of the group is provided with the access to the blockchain address of his or her group.

The lead researcher will only be able to revoke access via the interface which will call the revokeAccess() smart contract method in case one of the collaborators leaves the group. The revoked user is not in a position to recreate the corresponding CIDs even though the files are present in IPFS based on the contract. The blockchain ledger can be viewed to have any of such permission changes and their accountability and transparency are assured. The offered scenario shows how the system may facilitate the real cooperation and simultaneously maintain the rigid control of the access to some files.

VIII. Implementation and Results

The decentralized cloud storage model was achieved by the distributed file storage and a combination of blockchain smart contracts. The experiment is developed as a development environment, and it will be configured to use smart contracts to deploy, communicate with blockchain nodes, and store media files in IPFS. This part shall be the description of the tools, framework, and configurations that shall be utilized to construct and test the proposed architecture.

A. Simulation Process and Parameters

The suggested decentralized storage infrastructure was modeled and tested on the basis of a localized blockchain development environment. In particular, Hardhat framework was used to compile, test, and deploy the Solidity smart contracts to a local Ethereum test network. In the client interactions, a React.js frontend application was created, and the MetaMask was incorporated to support secure cryptographic wallets. In order to simulate the real-life decentralized storage behavior, Pinata API was utilized as the main IPFS pinning service. The simulation process has defined certain parameters of the network, such as a simulated block mining time of 12 seconds and a monitored gas limit to have a proper measure of computational costs.

B. Dataset Description

To strictly test the practical efficacy of the system, a standardized test data of multimedia files was built. This data set consisted of 50 varying sized image files (JPEG and PNG) with a size between 1 GB and 10 GB. These three file parameters have been chosen to accurately quantify IPFS upload latency, Content Identifier (CID) generation time, and future file retrieval efficiency at a range of network data loads.

C. Experimental Results and System Effectiveness

Recorded in the execution phase was the performance of the proposed architecture. It was also evident that the effective integration of IPFS unloaded the main blockchain ledger by storing heavy data thus reducing drastically the cost of the transactions. Moreover, access control, which is performed by smart contracts, was shown to be extremely innovative and productive. Upon selection of non-authorised user wallets, the blockchain protocol would automatically revert invalid retrieval attempts immediately, which is confirmation of the fact that zero unauthorized access to the off-chain data can be attained.

D. Performance Visualization

In order to get a better picture of how effective the system is in its functionality, the following are the summarized experimental metrics recorded. A performance table was created to demonstrate the relationship between file size, IPFS upload latency and costs of smart contract execution.

TABLE I
SYSTEM PERFORMANCE METRICS

File (MB)	Upload (ms)	Gas Cost (Gwei)	Retrieval (ms)
1.0	450	45,200	210
2.5	820	45,200	340
5.0	1450	45,200	580
10.0	2600	45,200	920

As visualized in Table I, it is demonstrated that the smart contract gas cost remains entirely constant (45,200 Gwei) regardless of the media file size. This data clearly validates the novelty and effectiveness of the proposed off-chain storage mechanism, as user processing fees are not negatively impacted by the scale of the uploaded media.

IX. RESULTS AND DISCUSSION

The proposed decentralized storage system was evaluated primarily on usability and the security of blockchain-based access controls. The system was working perfectly, users were able to upload images and store them in IPFS and generate their own CIDs and smart contracts did the permission work in the background. Finally, the findings demonstrate that it is possible to discontinue the use of large cloud vendors without damaging the data integrity and provide users with a real ownership of the digital assets.

A. Functional Outcomes

The following experiments proved that the system works as desired:

- Photos uploaded via the user interface were successfully stored in IPFS, with corresponding CIDs generated and stored on the blockchain.
- The smart contract successfully enforced ownership rules, ensuring permissions could only be granted or denied by the original uploader.
- Unauthorized users were effectively locked out, preventing confidential data retrieval.
- Public and private visibility modes functioned correctly, offering granular control when posting content.

B. Performance Analysis

The IPFS network load was the most significant factor in the testing that did not consider the blockchain when it comes to finding an image, and the time to find the image was taken into account. The median of the time to data access was acceptable in the real world use since earlier researchers concluded that IPFS could allow an efficient distribution of access to files [10], [11]. The metadata (CID) is solely stored in the blockchain which essentially means the overhead of storage was minimized which is in line with the principles of the decentralized system design that has been covered in the respective literature [2], [6].

C. Security and Access Control Evaluation

The blockchain registry ensured inherent documentation of access messages, which provided verifiable signals of the changes in permissions. The decentralized system had reduced the risks of having a single point of weakness compared with centralized architecture in which any data misuse between nodes could happen and external attacks may be experienced as observed in [1], [7], [14]. Unauthorized access attempts were automatically rejected, which proved that the smart contract logic can be used to implement the access control on a fine-grained level.

D. User Experience

The user interface abstracts the underlying complexities of the blockchain, so that any person can use the system, regardless of whether or not they have ever touched a decentralized application [6] . We overcame the usability problems of the previous storage systems which were complicated with a lot of pre-coded options to share or revoke access because we had the complex codes, which we substituted with simple dropdown menus. The ease of use of this data governance model is precisely what will make it stand out among others.

E. Overall Discussion

The results demonstrate that reliance on centralized service providers can be reduced to ensure the safety of our data. With a lean on blockchain and IPFS, we have created a model that is focused on user sovereignty - where you are the owner of your own data and which data you share with who. There

are drawbacks to decentralized networks, of course, in terms of speed, but it is a minor sacrifice to pay in order to have a system that you can actually trust. This is not merely a demonstration of concept; it has been a roadmap of how we can archive information in the actual world with a lot of security.

X. CONCLUSION AND FUTURE SCOPE

This paper successfully developed and test a decentralized cloud storage system that combines InterPlanetary File System (IPFS) and Solidity smart contracts successfully. By shifting from centralized data storage to a peer-to-peer network, inherent vulnerabilities such as single points of failure, privacy violations, and unauthorized access to data were effectively eliminated. The implementation process led to secure off-chain data hosting, and autonomous implementation of immutable access control policies through on-chain smart contracts. Moreover, granular control over permission, form of public and private visibility, was provided to the user in a seamless manner. As a result, the users regain full control over their data without any third party intermediaries.

As to the future of this study, a number of important improvements are suggested. To begin with, the native end-to-end encryption should be implemented to provide additional security to highly sensitive multimedia files prior to the IPFS pinning procedure. Also, the system will be extended to treat other types of document, audio and video files besides image files. Lastly, it is intended that this architecture will be deployed to a public blockchain mainnet and in conjunction with decentralized identity (DID) schemes, so that their scalability and the ability to be adopted on an enterprise-level globally can be comprehensively evaluated.

REFERENCES

[1] "Decentralized and Secure Access Control Model for Multi-Cloud Data Storage," *IIETA Journal*, 2025. DOI: 10.18280/ijsse.150203.

[2] M. R. Haque, S. Islam Munna, S. Ahmed, M. T. Islam, M. M. Hassan Onik, and A. A. Rahman, "An Integrated Blockchain and IPFS-Based Solution for Secure and Efficient Source Code Repository Hosting," *PLoS One*, 2025.

[3] S. R. Bandanadam *et al.*, "Decentralized Big Data Auditing Scheme for Cloud Storage Based on Blockchain with Adaptive EI-GAMAL and Gazelle Optimization," *Journal of Computer Communication and Cybernetics Engineering*, 2025.

[4] B. P. Chintal *et al.*, "Secure Decentralized Storage System Using Blockchain and IPFS," *SSRN Electronic Journal*, 2025.

[5] S. C. Prabanand *et al.*, "Advanced Financial Security System Using Smart Contract in Private Ethereum Consortium Blockchain," *Nature Scientific Reports*, 2025.

[6] S. Tafeem and S. Jennifer Mary, "Decentralized Cloud Storage Architecture Using Block Chain and Smart Contracts," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 2025.

[7] "Blockchain Security: Threats, Vulnerabilities and Countermeasures - A Review," *SSRN Electronic Journal*, 2025.

[8] G. Danezis *et al.*, "Walrus: An Efficient Decentralized Storage Network," *arXiv Preprint*, arXiv:2505.05370, 2025.

[9] A. R. Kandlakunta *et al.*, "Cloud-Based Blockchain Technology for Data Storage and Security," *SSRN Electronic Journal*, 2024.

[10] X. Cong *et al.*, "Research on IPFS Image Copyright Protection Method," *ScienceDirect*, 2024.

[11] W. Peng *et al.*, "An Efficient Blockchain-Based Framework for File Sharing," *Nature Scientific Reports*, 2024.

[12] S. Chaudhary *et al.*, "A Smart Contract and IPFS-Based Framework for Secure EV Synchronization at Charging Stations," *ScienceDirect*, 2024.

[13] A. A. G. Agung *et al.*, "Smart Contract and IPFS Decentralized Storage for Halal Certification Process," *Journal of Information Visualization (JOIV)*, 2024.

[14] "Blockchain-Based File Sharing System – A Hybrid Approach," *IRJMS*, 2024.

[15] H. S. Musa *et al.*, "Survey on Blockchain-Based Data Storage Security for Mobile Applications," *PubMed Central (PMC)*, 2023.

[16] S. Ray, K. N. Mishra, and S. Dutta, "Security Enhancements in M-Health Using Distributed Ledger Technology based Digital Locker System," *International Journal of Information Technology*, vol. 16, pp. 4253-4271, 2024.

[17] A. Kumar *et al.*, "Mapping the trajectory of blockchain technology and non-fungible tokens: a comprehensive bibliometric analysis," *International Journal of Information Technology*, 2024. DOI: 10.1007/s41870-024-02204-2.