Grenze International Journal of Engineering and Technology, June Issue

Blockchain Enabled Cloud Data Storage

Sofiya Khanam[1] and Syed Rehan[2]
[1-2]Department of Computer Science and Engineering, Anjuman College of Engineering Nagpur, Maharashtra, India
Email: sofiya.khanam2401@gmail.com, srehan@anjumanengg.edu.in

***Abstract*— Enabled Cloud Data Storage, the introduction of blockchain technologies can serve as an effective means of solving the existing problems related to security, data transparency, reliability of cloud storage. The current centralized models for cloud storage have multiple problems like the vulnerability to data breaches, having a single point of failure, inability to ensure data control to the users. To cope with these challenges, the proposed solution is the combination of IPFS with Ethereum and smart contracts as a way to develop a secure and effective cloud storage service. In the new proposed system, the clients will encrypt their files and upload to IPFS, while information about the ownership and access permissions will be stored in the blockchain. Smart contracts will be used to ensure the access control and data protection without having to use any intermediators. In addition, the system will be able to store small files entirely within the blockchain and large ones partially. However, even if there are some difficulties with the scalability, cost, and retrieval time in such a system, the proposed cloud storage is more advantageous than the existing solutions because of increased security and better performance.**

***Index Terms*— Cloud Storage, IPFS, Decentralization, Smart Contracts, Data Security, Ethereum, File Integrity.**

I. INTRODUCTION

Today, in a digital world, data has been one of the most prized possessions, which in turn has been the main source of innovations in various areas such as health care, finance, education, and technology. The exponential increase in digital data has made the need for secure, reliable, and scalable cloud storage solutions even higher as well. Centralized traditional cloud storage systems such as Google Drive, Amazon Web Services (AWS), and Dropbox have been the main providers for the internet and have been very important to the accessibility and sharing of data.

The proposed solution entails the adoption of the Interplanetary File System (IPFS) for decentralized storage of files and at the same time the Ethereum blockchain for keeping unchangeable records and smart contract-based control of access. IPFS permits the storage of the content in an address-based manner; thus, files can be fetched using their hash values instead of physical locations, consequently, guaranteeing the authenticity of the data. Smart contracts operate in an automated manner to perform important processes such as registering files, granting permissions, handling payments, and transferring property rights, and all these are possible without any involvement from third parties. This paper discusses a cloud storage design using Ethereum and IPFS, focusing on its security and decentralized nature, while also identifying its potential difficulties, restrictions, and improvements.

Grenze ID: 01.GIJET.12.2.133_22

II. Objectives

- Objective of this research is to develop a decentralized cloud storage system using blockchain and IPFS to eliminate any potential point of failures.
- Apart from this, one more objective is to ensure the security and confidentiality of data through encryption and blockchain technology.
- This work also aims to automate data access control, ownership verification, and transaction management using smart contracts without third-party intermediaries.
- Finally, the system seeks to improve storage efficiency and cost-effectiveness by storing large files off-chain in IPFS while maintaining essential metadata on the blockchain.

III. Related Work

A. Traditional Cloud Storage Systems

Google Drive, Dropbox, and Amazon Web Services (AWS) are the typical cloud storage models that prove to be extremely popular in terms of scalability in data storage and accesses. Still, all these technologies are centralized and consequently vulnerable to data breaches, hacking, and single point of failure [1]. The centralized platforms are faced with challenges related to transparency and compliance issues, besides, experiencing enormous expenses; as a result, they cannot keep pace with the fast growth of data amounts [2]. In contrast, decentralized alternatives are gaining more and more popularity due to the forecast that 2024 might become a turning point when companies will switch from centralized to decentralized cloud platforms [3]. The benefits associated with traditional cloud providers include convenience and elasticity, but at the same time, their users face the issue of losing sovereignty since they are unable to guarantee data consistency or manage encryption keys [4]. Such an obstacle becomes a catalyst for researching alternative technologies that would provide equal levels of security along with building trust between nodes in the case of confidential data handling [5].

B. Blockchain for Data Integrity and Access Control

The blockchain technology guarantees all the core features of immutability, transparency, and decentralization, which make it the right choice for the enhancement of data integrity in cloud systems. Blockchain, as it were, keeps a distributed ledger of every transaction or metadata update that not only makes it unbelievably but also practically impossible to alter or carry out unauthorized modifications [6]. A number of scientific publications have come with the similar conclusion that a deployment of blockchain in cloud computing infrastructures leads to the de facto increased visibility and auditing of data within the system [7]. An innovative storage solution proposed by Merlec and In in 2024 awarded user-oriented data self-sovereignty, that is the control of every access policy belongs to the records on the chain [8]. However, recent investigations have brought to light the possible application of blockchain for sophisticated access control through smart contracts [9]. On the other hand, hurdles such as scalability and energy consumption have to be overcome [10]. Even though these drawbacks exist, blockchain-based data integrity frameworks are radically transforming the structure of secure cloud environments by diminishing intermediaries thus making it possible for the users and the providers to have trusted verification without having trust relationships [11].

C. Decentralized Storage Systems and IPFS

Interplanetary File System (IPFS) is a highly advanced peer-to-peer technology that is among the most effective technologies used for storing information on a decentralized basis. Unlike traditional technologies, which work based on location searching, IPFS works using content addressing, meaning that each file is identified by its unique hash (CID) [12]. The technology offers the benefit of having three features at once: availability, authentication, and redundancy because users can access files from various locations. In 2024, the researchers conducted extensive research about decentralized storage, proving that the use of IPFS alongside blockchain metadata can greatly enhance the security of data stored in such a manner and increase performance [13]. Moreover, IPFS helps establish a connection between Filecoin to store and retrieve data with bonuses [14]. Currently, the main limitations of the technology include high retrieval latency, node failures, and network congestion [15]. Although there are several disadvantages associated with IPFS, the integration of this technology into blockchain systems becomes increasingly popular and affordable.

D. Blockchain-Based Storage Platforms and Incentives

Current blockchain-based storage solutions, like Filecoin, Sia, Arweave, and Storj, employ token economies to ensure fair data storage and retrieval. In these systems, the storage nodes earn money by providing proof of the storage of data using cryptographic proof mechanisms such as PoRep and PoSt [16, 17]. Blockchain storage services combined with the Interplanetary File System (IPFS) created a sustainable ecosystem for storage providers through Protocol Labs' Filecoin [18]. According to research in 2024, BFT storage systems have emerged in the market as a more reliable and rewarding option [19]. However, such systems experience problems with the volatility of tokens and governance challenges, although they are transparent and verifiable [20]. Despite these difficulties, incentive-based blockchain storage systems continue to develop into a safer and decentralized solution that ensures high fault tolerance and reduces dependency on centralized clouds [8].

E. Smart Contracts for Automation and Governance

The smart contract technology is what makes the automation of the blockchain-based storage systems possible. The smart contracts perform operations regarding the file such as registering the files, managing their ownership, and providing access to certain individuals depending on the specified conditions without any human mediation [9]. In one of its examples, Kandlakunta and Simuni (2024) showed how the smart contract technology could be used for performing permission and payment procedures automatically during the cloud-blockchain integration of data governance [3]. Smart contracts can automate processes in such a way that they not only give users the opportunity to regulate the access but also allow the transactions to occur within specific rules [10]. However, the problem that arises from immutability is that once there is an error in the deployed code, it will remain forever; hence, the importance of designing auditable and upgradeable contracts [7]. The latest advancements in the blockchain-based frameworks suggest creating hybrid solutions in which the smart contracts work together with the oracles outside the chain. In other words, the system remains flexible due to off-chain oracles, but the security of the blockchain is preserved [6].

F. Security, Privacy, and Compliance

The primary aspects that should be considered in decentralized storage architectures remain security and privacy. Trust increases with blockchain technology-based approaches, however, other challenges including data privacy, encryption management, and legal considerations emerge [5]. An approach to ensuring high-level protection in the process using cryptographic algorithms of AES, RSA, and SHA-256 combined with blockchain was proposed by researchers [4]. In 2024, Zhou et al. introduced the concept of Haina Storage which included blockchain as well as dynamic lock and proof-of-resource for increasing fairness and efficiency of the system [15]. Moreover, zero-knowledge proof (ZKP) technologies and advent of post-quantum cryptography may become the next stage for privacy-preserving storage [11]. Nevertheless, the problems related to right to erasure according to GDPR requirements as well as data localization are left open issues [2]. Transition of these challenges into privacy-aware smart contracts and metadata encryption sharing can be considered as promising solutions for increasing user confidence towards decentralized storage architecture [9].

G. Research Gaps and Motivation

All the studies cited earlier confirm that the capabilities of the blockchain technology-enabled cloud storage system have grown enough to overcome the limitations of the present systems. The combination of decentralized information storage, encryption technology, and automatic programming is what makes such systems the perfect combination of safety, transparency, and reliability [8]. However, at the same time, the issues associated with scalability, huge transaction costs, interoperability, and usability remain major barriers for their mass adoption [6]. In order to help this, the researchers propose improving the consensus algorithms, using layer-2 technologies for scalability, and having AI-based monitoring for data availability and retrieval [13]. Likewise, legal and environmental factors need to be considered to ensure compliance and to be able to call the process eco-friendly [1]. The goal of the current project is to remove these obstacles by developing a hybrid blockchain-IPFS framework that will not only make data access easier, but also faster, and provide a proof of verifiable storage ownership via smart contracts and decentralized indexing techniques [4]. It is these gaps that give rise to the proposed blockchain–IPFS-based cloud storage framework that this paper discusses.

The architecture of the suggested blockchain-based cloud storage system is illustrated in Figure 1. The system consists of four main components: Client, IPFS, Blockchain Network, and Smart Contracts. To begin with, the client encrypts the files and uploads them to the IPFS network, which then stores the files in a distributed manner and assigns them a unique content identifier (CID). The CID and the file metadata which include ownership and access rights are sent to the blockchain using smart contracts. This is because the smart contracts automate the procedures of access control, proof of ownership, and transactions. Then, the encrypted files are gathered by the authorized users on the IPFS network, and the data validation process takes place using the records stored on the blockchain network. This system ensures that there is no presence of any central server, which means that decentralization and security of data access take place through this architecture.

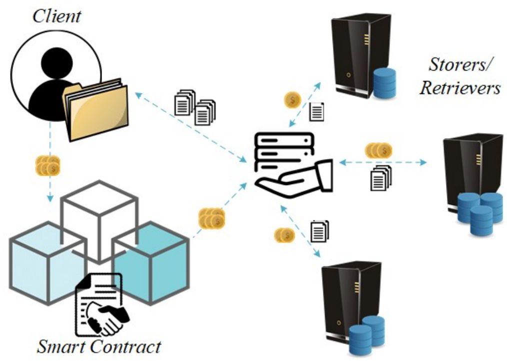

Figure 1: Architecture of Blockchain-Based Cloud Storage System

III. Proposed Blockchain-based Cloud Storage System

First of all, the proposed blockchain-based cloud storage solution combines not only the use of both distributed storage and distributed ledgers but also adds data security, data ownership, and transparency on a new level. Unlike conventional centralized cloud storage solutions, the proposed one differs significantly in that the encrypted data chunks are stored in several nodes at once making it robust to any possible malfunctions. The smart contracts manage to perform such functions as controlling access, ensuring the proof of ownership, and tracking the transactions and thus there is no need to rely upon any intermediaries anymore. Moreover, all the information regarding file ownership and file integrity hashes is stored on the blockchain providing an immutable proof while being simultaneously open to access. The Inter Planetary File System (IPFS), used in conjunction with distributed storage, adds to the latter's reliability by allowing to retrieve files based on cryptographic hashes rather than locations. Despite the advantages, there are still several problems concerning scalability, retrieving latency, and regulation compliance that will be further addressed (Table I).

A. System Workflow

- The user encrypts the data locally before uploading to ensure confidentiality.
- The encrypted file is uploaded to the Interplanetary File System (IPFS), which generates a unique Content Identifier (CID) based on the file's content.
- The generated CID along with file metadata such as ownership and access permissions is recorded on the blockchain through smart contracts.
- Smart contracts automatically enforce access control policies and verify file ownership without relying on third-party intermediaries.
- Authorized users retrieve the encrypted file from IPFS and validate its integrity by comparing the file hash with the blockchain-stored records.

TABLE I: Comparison of Proposed Blockchain-based Storage with Traditional Cloud Storage

Feature / Parameter	Proposed Blockchain-Based Cloud Storage	AWS / Dropbox (Traditional Cloud Storage)
Storage Model	Decentralized storage using IPFS	Centralized storage managed by a single provider
Data Control & Ownership	User retains full ownership and control of data	Data controlled by cloud service provider
Security Mechanism	Client-side encryption + blockchain immutability	Server-side encryption managed by provider
Data Integrity Verification	Cryptographic hashes stored on blockchain enable tamper detection	Integrity verification handled internally by provider
Single Point of Failure	No single point of failure due to distributed nodes	Vulnerable to outages and centralized failures
Transparency & Auditability	Fully transparent and auditable via blockchain ledger	Limited transparency; users must trust provider
Access Control	Smart contracts enforce automated access control	Access controlled by centralized authentication systems
Data Availability	High availability through distributed IPFS nodes	High availability but dependent on provider infrastructure

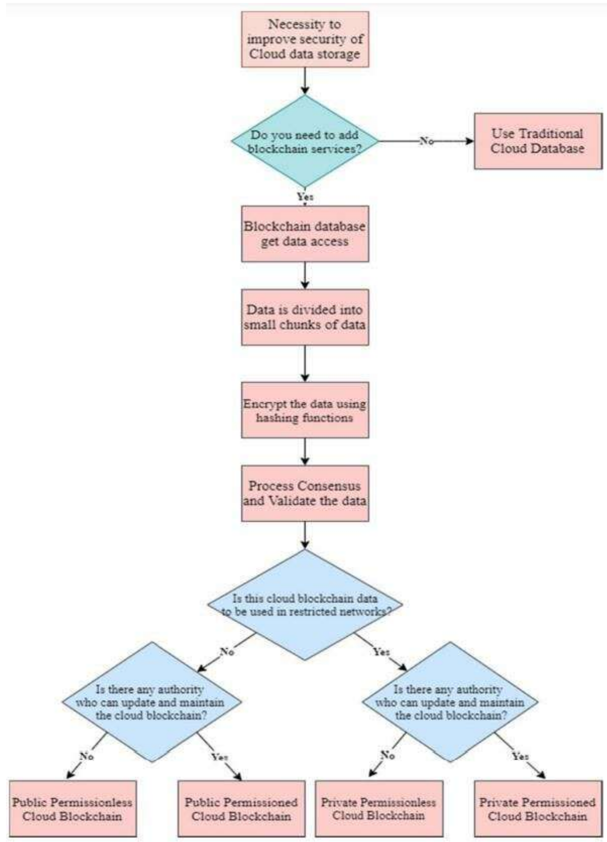

Figure 2. Flowchart of Blockchain-Based Cloud Storage Decision Process

Figure 2. Flowchart of Blockchain-Based Cloud Storage Decision Process illustrates the procedure of using blockchain in cloud storage for data. It starts with identifying the need for better data security in the cloud. If there is no need for blockchain, the classic cloud database is adopted. On the contrary, if it is mandatory to integrate a blockchain, the technology proceeds by granting access to the blockchain database to the data. After that, the data is cut into smaller pieces which improves redundancy and fault tolerance. Each piece of data is encrypted with hashing functions so that its integrity and confidentiality are protected. Further, a consensus mechanism is implemented to verify transactions throughout the blockchain, which in turn validates the data and eliminates the possibility of it being altered. The next step is to choose between a private (restricted) or a public (open) setting for the blockchain to function. Finally, the categorization was made into four models - Public Permissionless Cloud Blockchain, Public Permissioned Cloud Blockchain, Private Permissionless Cloud Blockchain, or Private Permissioned Cloud Blockchain - based on the presence of an authority that controls the updates.

IV. Methodology

The blockchain-enabled cloud storage system's methodology proposed consists of a hybrid architecture that integrates the blockchain technology with decentralized storage technology via the Interplanetary File System (IPFS). The proposed approach is to improve the security, transparency, and fault tolerance of data while it already gets rid of centralized cloud solutions. The data processing takes place at the client-side in the first instance, and then the files are encrypted to guarantee confidentiality before they are actually stored. The storage nodes may be compromised but the data will not be accessible to unauthorized persons. After that, the encrypted file is sent to the IPFS where it gets divided and stored in different places corresponding to the decentralized nodes. The IPFS assigns a unique Content Identifier (CID) to each file based on its cryptographic hash that allows, therefore, for content-based addressing and integrity verification to take place. Next, the newly created CID as well as the file metadata consisting of ownership information, access permissions, and timestamps is stored on the blockchain through the use of smart contracts. The blockchain serves as a permanent and unchangeable ledger that not only protects metadata but also allows users to see and trace the transaction. Smart contracts automatically handle very important processes like file registration, authorizations for access, ownership validation, and logging of transactions, thus making it unnecessary to have reliable third-party mediators. When a user asks to access a file, the smart contract checks the user's right to access the file according to the previously set rules of access control. After that, the user gets the encrypted file from IPFS and checks its correctness by matching the hash of the retrieved file with the hash of the one stored in the blockchain (CID). This process ensures that the data has not been altered during storage or transmission (Table II).

TABLE II. OVERVIEW OF ISSUES APPROACHES, METHODS

No. / Reference	Issue Discussed	Approach & Method
[1] Merlec & In (2024)	Centralized storage limits user data sovereignty and transparency.	Proposed decentralized blockchain-based storage enabling data self-sovereignty through immutable ledgers and distributed governance mechanisms.
[2] Onuora et al. (2024)	Lack of scalability and high dependency on centralized control in traditional clouds.	Conducted a comprehensive review of decentralized cloud models and suggested hybrid blockchain–IPFS integration for secure, scalable storage.
[3] Kandlakunta & Simuni (2024)	Data security and integrity risks in conventional cloud systems.	Developed a blockchain–cloud integration framework using smart contracts to automate secure storage and verification.
[4] Zhou et al. (2024)	Inefficiency and fairness in blockchain-based storage mechanisms.	Designed Haina Storage, an improved blockchain framework using dynamic resource allocation and proof-of-resource validation for efficiency.
[5] He (2024)	Limitations in contract-based and network-based blockchain systems.	Performed comparative analysis on blockchain network structures and contract models to identify optimal architecture for decentralized data storage.
[6] Dadkhah et al. (2024)	Storing big data efficiently within consortium blockchain environments.	Proposed DBNode, a decentralized big data storage model ensuring fault tolerance and integrity in consortium blockchain settings.
[7] Guo et al. (2024)	Byzantine faults and reliability issues in decentralized storage systems.	Introduced BFT-DSN, a Byzantine Fault Tolerant network improving resilience and ensuring secure communication between distributed storage nodes.
[8] Protocol Labs (2024)	Lack of incentive for long-term decentralized data storage.	Developed Filecoin, a token-based blockchain storage network using Proof-of-Replication and Proof-of-Spacetime for verifiable storage.
[9] Shanti Guru et al. (2024)	Security challenges and data redundancy management in decentralized storage.	Implemented blockchain and IPFS integration with cryptographic hashing to enhance security and reduce redundancy in distributed storage.
[10] GMI Insights (2024)	Growing demand for decentralized storage markets and enterprise adoption barriers.	Analyzed decentralized market growth and emphasized the importance of interoperable and sustainable blockchain storage infrastructures.
[11] Chen & Xu (2025)	Privacy preservation in blockchain-enabled cloud storage.	Proposed a privacy-preserving encryption mechanism integrating blockchain and symmetric cryptography for secure data sharing.
[12] Singh et al. (2025)	Integration complexity between IPFS and blockchain networks.	Designed a secure IPFS–blockchain integration model ensuring data immutability, efficient access, and decentralized retrieval verification.
[13] Patel & Agarwal (2025)	Inefficient node selection and slow retrieval in decentralized networks.	Applied AI-assisted algorithms to optimize storage node selection and enhance overall retrieval speed and efficiency.
[14] Prakash et al. (2024)	Scalability and throughput issues in public blockchain storage systems.	Proposed hybrid blockchain architecture combining private and public layers for improved scalability and transaction speed.
[15] Li et al. (2025)	Trade-offs between security and efficiency in decentralized systems.	Analyzed security–efficiency balance and recommended optimized consensus protocols for faster, more secure data handling.
[16] Kumar & Thomas (2025)	Challenges in IPFS-based decentralized file storage models.	Explored IPFS implementation details and performance benchmarks, suggesting enhancements for latency and storage management.
[17] Lee & Choi (2025)	Lack of economic incentives for decentralized node participation.	Proposed tokenized incentive mechanisms to reward active nodes and maintain reliable storage networks.

[18] Zhang & Liu (2024)	Scalability constraints in blockchain-based cloud infrastructures.	Introduced architectural improvements to enhance transaction throughput and reduce network congestion.
[19] Luo & Yu (2025)	High energy consumption in consensus algorithms.	Proposed energy-efficient blockchain consensus (PoA and DPoS) models for sustainable decentralized storage systems.
[20] Das & Srivastava (2025)	Vulnerabilities in smart contracts managing cloud data storage.	Conducted vulnerability analysis and proposed security frameworks to prevent exploits and ensure safe smart contract deployment.

V. Framework Design

The architecture of the system is designed in a way that there are five layers which constitute the most important elements, namely User Layer, Application Layer, Blockchain Layer, Storage Layer, and Security Layer, and since these layers serve different purposes, this makes the functioning of the system smooth and effective.

A. User Layer

This layer serves as the interface between the system and the end-users. The users can through a secure and easy-to-use web or mobile interface upload, retrieve or manage their files. It also manages user authentication via blockchain wallets such as MetaMask which provides secure login and transaction signing.

B. Application Layer

The application layer is the one that oversees the coordination of the user interface and the blockchain network. This layer manages users' requests, performs the smart contracts, and communicates with the IPFS nodes. It offers APIs for activities such as file uploads, metadata management, and transaction verification, which ensures proper interaction between the different modules.

C. Blockchain Layer

The backbone of the framework, this layer operates an unchangeable ledger that logs file metadata, ownership, timestamps, and access permissions. It is here that the smart contracts are executed for the automation of the main operations such as registration, control of access,

D. Storage Layer

The Interplanetary File System (IPFS) is the technology that the second layer uses for decentralized storage of files. Firstly, files are encrypted, then divided into parts, and finally, sent to different nodes that are cooperating within the network.
Each piece of the file is given a distinct Content Identifier (CID) which is then logged on the blockchain for the purpose of integrity certification. This layer is supplying fault tolerance, multiple copies, and quick access without the need of a central server.

E. Security Layer

Security involves encryption, hashing, and access control policies. The encryption of the client-side takes place before the file is uploaded, and the file's hash is recorded on the blockchain to detect any unauthorized changes. Public key cryptography guarantees that only the correct users can decrypt and get access to the data, hence, the data is kept private and confidential.

V. Results and Discussion

A. Security Discussion

The proposed blockchain-based cloud storage system offers a significant increase in data security through the combination of encryption and blockchain inaccessibility. The files are encrypted by the client before they are uploaded, thus keeping the information secret even if the storage nodes are compromised. The blockchain has made it infeasible to change the records of file metadata and cryptographic hashes, consequently, no unauthorized changes can be made and integrity verification is highly reliable. Moreover, smart contracts provide an additional layer of security by automatically issuing and confirming access and ownership, thus, reducing the need for intermediaries.
Accordingly, the system provides a superior level of security compared to regular centralized cloud storage systems by dealing with the issues of data tampering, unauthorized access, and single points of failure in a more effective manner.

B. Performance Discussion

Storing large data files on IPFS off-chain and only their metadata on the blockchain results in a considerable reduction of both storage costs and blockchain overhead. The hybrid model improves scalability by taking on-chain data storage and transaction size down to the minimum possible level. However, the reliance on IPFS' decentralized storage may result in longer retrieval times, especially in cases where the storage nodes are located far apart or one of them is down, when compared to centralized cloud servers. Nonetheless, the system is able to come up with an effective trade-off among cost savings, data integrity, and the availability of decentralized data.

VI. Challenges and Limitation

A. Scalability Issues

Scalability The principal problems that hinder blockchain networks are limited transaction throughput and high latency. The growth of users and documents results in traffic on the blockchain which, in turn, slows down data verification and raises transaction costs. Even now, next-generation consensus mechanisms like Proof-of-Work (PoW) and Proof-of-Stake (PoS) are still not optimally suited for heavy file storage operations.

B. High Storage and Computation Costs

The process of storing huge data sets on the blockchain is expensive and not very practical. Despite the fact that IPFS and similar systems keep data off-chain, on-chain activities (such as smart contract execution, metadata storage) still have gas fees attached that vary with network traffic. This picture of a highly ineffective scenario tells us that decentralized storage becomes less cost-efficient for large organizations, compared to centralized cloud storage.

C. Data Retrieval Latency

One of the drawbacks of peer-to-peer networks is that they are distributed which results in longer file retrieval compared to centralized cloud systems, especially in cases where some storage nodes are offline or in distant geographical regions. This affects time-dependent applications that need quick access to data.

D. Security and Privacy Concerns

The feature of blockchain being unchangeable is a major benefit but the drawback is that confidentiality of the data can only be achieved through encryption. If the management of keys is not up to par or if the keys for encryption are leaked, then the secret data becomes public. Moreover, it is quite a technical problem to guarantee the privacy of the user while being transparent on a public blockchain at the same time.

E. Regulatory and Legal Issues

The immutable feature of blockchain technology has direct conflict with some data protection laws, for example, the GDPR's "right to be forgotten."
Another issue is the jurisdictional conflict when small chunks of data are spread across different countries, each with its own legal system. It is still up in the air who is liable and who the data owner is in decentralized networks.

F. Energy Consumption

The consumption of a huge amount of energy is one of the characteristics of blockchain networks, especially those using heavy energy consensus mechanisms such as PoW. Environmental concerns come along with this power consumption and furthermore, the applicability of such systems for the continuous process of data storage and retrieval is restricted due to power consumption.

VII. Future Enhancement

A. AI Integration

The partnership between Artificial Intelligence (AI) and blockchain-based cloud storage can result in the faster and smarter choosing of storage nodes, forecasting of data access, and instant file retrieval. Furthermore, AI-powered monitoring could play a significant role in the even distribution of storage among the decentralized nodes, thereby reducing latency and detecting very early on abnormal behaviors like unreliable or malicious nodes. Through its intelligent management of the network resources, AI could enhance the performance, reliability, and scalability of the system while simultaneously reducing energy consumption.

B. Layer-2 and Sidechain Solutions

Scalability plus transaction cost reduction are the great impacts of the application of Layer-2 solutions and sidechains to the existing system. Besides, this set of technologies completely soothes the difficulty of network congestion but also lower the gas fees by carrying out transactions outside the main chain and guaranteeing security through the periodic anchoring of the blockchain. The great compatibility of Layer-2 technologies allows for the faster confirmation of transactions and the smoother user experience which is achieved by not compromising the immutability and integrity of the blockchain-based storage operations.

C. Interoperability

It is essential for future research to investigate the interoperability between the different blockchains as well as the traditional cloud storage systems. Interoperable frameworks will allow seamless data transfer, data sharing, and authentication between these systems, making such processes more flexible and reducing the need for a single provider. Moreover, this will lead to an increase in the adoption of the technology by the general public and hybrid cloud storage systems.

VIII. CONCLUSION

Blockchain Technology-Based Cloud Storage System can be seen as a more secure and decentralized option, as it relies on blockchain and IPFS technologies, ensuring the safety and integrity of data, confidentiality, and transparency. All data stored in the new system is encrypted, verified, and distributed across nodes, which makes all vulnerabilities impossible for this system. In addition to that, all operations dealing with data modification, manipulation, transfer, and usage are performed via smart contracts. Such elements make the proposed system more credible and reliable, but transaction delay and lack of scalability issues arise. Yet, future innovations and developments will solve these problems, as AI technologies and Layer-2 solutions could be applied to such systems.

ACKNOWLEDGMENT

On behalf of Ms. Sofiya Khanam and Prof. Syed Rehan, we would like to convey our heartfelt appreciation to the Department of Computer Science & Engineering, Anjuman College of Engineering, Nagpur, Maharashtra, India, for the required facilities and assistance provided to undertake this research.

REFERENCES

[1] M. M. Merlec and H. P. In, “Blockchain-Based Decentralized Storage Systems for Sustainable Data Self-Sovereignty: A Comparative Study,” Sustainability, vol. 16, no. 17, 2024.
[2] A. C. Onuora et al., “Decentralized Cloud Storage: A Comprehensive Review,” ResearchGate, 2024.
[3] A. R. Kandlakunta and G. Simuni, “Cloud-Based Blockchain Technology for Data Storage and Security,” SSRN, 2024.
[4] Z. Zhou et al., “Haina Storage: A Decentralized Secure Storage Framework Based on Improved Blockchain Structure,” arXiv preprint arXiv:2404.01606, 2024.
[5] L. He, “Comparative Examination of Network and Contract-Based Blockchain Storage Solutions,” arXiv preprint arXiv:2401.07417, 2024.
[6] N. Dadkhah et al., “DBNode: A Decentralized Storage System for Big Data in Consortium Blockchains,” arXiv preprint arXiv:2409.20123, 2024.
[7] H. Guo et al., “BFT-DSN: A Byzantine Fault Tolerant Decentralized Storage Network,” arXiv preprint arXiv:2402.12889, 2024.
[8] Protocol Labs, “Filecoin: A Decentralized Storage Network,” Whitepaper, 2024.
[9] Shanti Guru et al., “Blockchain Based Decentralized Storage System,” IJRASET, vol. 12, Mar. 2024.
[10] GMI Insights, “Decentralized Storage Market Size Report 2025–2034,” GMI Publications, 2024.
[11] Y. Chen and X. Xu, “Privacy-Preserving Cloud Storage via Blockchain-Based Encryption,” IEEE Access, vol. 12, pp. 25461–25474, 2025.
[12] A. Singh et al., “Integration of IPFS and Blockchain for Secure Cloud Storage,” Future Internet, vol. 17, no. 4, 2025.
[13] R. Patel and P. Agarwal, “Optimizing Decentralized Storage Using AI-Assisted Node Selection,” Sensors, vol. 25, no. 3, 2025.
[14] V. Prakash et al., “Hybrid Blockchain Models for Scalable Cloud Data Storage,” Journal of Cloud Computing, 2024.
[15] P. Li et al., “Security and Efficiency Trade-offs in Decentralized Storage,” IEEE Transactions on Cloud Computing, 2025.
[16] S. Kumar and R. Thomas, “A Study on IPFS-Based Decentralized File Systems,” Computers, vol. 13, no. 2, 2025.
[17] J. Lee and D. Choi, “Tokenized Incentive Models in Blockchain Storage,” IEEE Blockchain Letters, vol. 1, 2025.

[18] H. Zhang and C. Liu, "Scalability of Blockchain-Based Cloud Infrastructures," Computer Networks, vol. 240, 2024.
[19] X. Luo and F. Yu, "Energy-Efficient Consensus for Decentralized Storage," Sustainability, vol. 17, no. 9, 2025.
[20] K. J. Das and N. Srivastava, "Smart Contract Vulnerabilities in Cloud Storage Applications," IEEE Access, vol. 13, pp. 12094–12105, 2025.