Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

IPFS-Based Blockchain Solution for Secure and Efficient Data Sharing

Poonam Kumari [1], Meeta Singh[2]
[1,2] *Department of Computer Science and Engineering, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India*
pnmdv211@gmail.com, meeta.sangwan@gmail.com

ARTICLE INFO

Received: 24 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

This study introduces a decentralized blockchain-based framework for secure data exchange within cloud environments. It employs IPFS to encrypt and fragment files into multiple hash codes, enhancing security. Access is restricted to registered cloud users, ensuring controlled data distribution. Blockchain technology upholds data integrity by securely logging transactions, making them tamper-resistant. Unlike centralized storage models, this decentralized approach eliminates single points of failure, improving reliability and security. By spreading data across multiple nodes, the system reduces risks from cyber threats and unreliable cloud providers. It also lowers computational and communication overhead, ensuring efficient data transfer. Additionally, it protects sensitive data from unauthorized breaches and cyber-attacks. The blockchain-IPFS fusion strengthens security and accessibility, allowing seamless, regulated data handling across diverse domains. Tailored to counter security challenges in cloud storage, the system ensures data confidentiality, controlled sharing, and restricted access. Its decentralized design fosters transparency, minimizes dependence on centralized entities, and mitigates security flaws. By utilizing blockchain's immutable nature and cryptographic measures, this system enhances trust and ensures a fortified environment for data transactions. It mitigates risks linked to conventional cloud storage, offering resilience against data loss and cyber hazards. The system is optimized for performance, reducing latency and improving accessibility. Scalability is a key feature, supporting growing data storage demands. It guarantees data confidentiality, integrity, and availability, fostering secure cross-domain data sharing. Ultimately, this framework creates a secure, efficient, and decentralized solution for cloud storage and transfer, advancing data protection and accessibility.

Keywords: Blockchain, Cloud storage, Ethereum , Interplanetary File System (IPFS).

INTRODUCTION

While cloud providers strive to make data sharing convenient, significant security concerns remain, particularly regarding the reliability of cloud service providers. These providers are vulnerable not only to external cyber-attacks but also to internal threats from malicious employees, posing serious risks to cloud data security [5]. Encryption is commonly used to ensure secure data access however, managing access rights to encrypted data is a significant challenge. A good solution is Cipher-text Policy Feature-Based Encryption (CP-ABE), which enables access to secure data in cloud storage [1]. However, Many CP-ABE schemes focus on a single authority, which limits access and is more complex because attributes are shared across multiple domains and trust entities. To address this, Chase (2007) proposed the original multi-authority CP-ABE approach where different authorities manage different sectors, reducing reliance on a single agency. Despite various proposed extensions, the single-point failure issue remains prevalent in centralized systems [2]. Division of specialist areas into different subgroups, each of which is regulated by a different authority, continues to highlight the centralization problem.

As more data is stored on cloud services, preserving its privacy and security becomes a critical concern. To safeguard data, it is typically stored in the form of cipher-text, requiring a third-party access key when a user requests access [6]. However, if the third-party is untrustworthy, the system's security can be compromised. The best way to solve this problem is to use a decentralized system, such as a block-chain, which creates a database with multiple authorities for information exchange [3]. Block-chain's decentralized nature, along with its openness, autonomy, and independence from a central trusted authority, offers enhanced security. By leveraging encryption, block-chain can preserve anonymity and provide greater security compared to traditional data storage methods. The integration of block-chain with

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

cloud data sharing systems holds significant potential for addressing challenges related to secure data access within a decentralized multi-authority model [4]. Block-chain technology is increasingly being adopted for access control in various applications due to its key properties, such as immutability, durability, audit-ability, and dependability. These features make block-chain an ideal complement to access control solutions, ensuring transaction transparency while supporting privacy and secure data management. Block-chain records all transactions and data on all participating peers, further enhancing security and accountability.

Problem Statement

Cloud servers, which function as centralized authorities, store vast amounts of data. However, centralization brings significant risks, notably the issue of a single point of failure. To mitigate this, many managers proposed a hierarchical architecture in which the central authority is divided into domain organizations, reducing the likelihood of such failures. Many existing attribute-based encryption schemes rely on a single central authority to manage user attributes, making them vulnerable to a single point of failure. In response, several multi-authority CP-ABE methods have been developed, but they still face challenges, so really cool data processing and communication costs for users. To overcome these limitations, we recommend that the development system uses block-chain and IPFS, enabling efficient and secure access to cloud data by multiple authorities. Block-chain technology ensures a permanent, clear record of vendor and user agreements.Users can request data from the owner after accepting the terms recorded on the block-chain, thereby enhancing transparency, accountability, and providing fine-grained access control for research data.

LITERATURE SURVEY

IPFS-based blockchain data storage architecture helps overcome the storage limits of traditional blockchains by utilizing a distributed file system. IPFS (Inter Planetary File System) divides data into chunks and stores them across multiple nodes in a peer-to-peer network, ensuring that each file is uniquely identified using content-addressing. The user controls access to the data by providing the path to retrieve each chunk, ensuring efficient storage and enhanced security. This model is ideal for securely uploading, reading, and downloading documents [7].Developed registered card verification system with distributed ledger technology Ethereum block chain for building decentralized applications powered by smart contracts. This system categorizes users into three roles: certification units responsible for issuing and managing certificates, students who receive and access their credentials upon meeting specific criteria, and service providers tasked with system maintenance. However, the limitation of this approach is that it relies on a hash value, which is publicly known and potentially compromises security [8]. To address blockchain storage limitations, an IPFS was a block-based data storage architecture that was introduced. IPFS (Interplanetary File System) uses a peer-to-peer model for sharing and storing data, dividing uploaded files into chunks distributed across its network. Each chunk is identified through a content-addressed global names pace, and access to document paths is exclusive to the user. This approach enhances data storage efficiency and security, making it suitable for document uploading, retrieval, and downloading [9].Furthermore, an analysis of Ethereum blockchain clients, including Geth and Parity, reveals significant performance differences. Transactions on a private Ethereum blockchain using the Parity client were observed to be 89.8% faster on average for transaction sets ranging from 1,000 to 10,000 compared to the Geth client under identical system configurations. These findings highlight the impact of client selection on Ethereum performance [10].This paper explores image watermarking using Computation-based secret sharing is simple, semi-complete. By employing this strategy, the paper enables the validation of ownership through RGB watermarking, even in cases where portions of the image file are disrupted. Unlike traditional random-stream watermarking schemes, this approach supports lightweight, semi-complete verification, providing a unique advantage. The proposed method has been tested and compared with other state-of-the-art techniques [11]. Additionally, this paper proposes an Arabic e-text watermarking technique that supports partial anonymity using number-based secret sharing. The approach utilizes the Arabic "Kashida" character to embed watermarking data. This technique ensures full security for hiding watermarking bits, eliminating the need to directly conceal secrets as seen in previous methods. A password is required to access the account is a secret search function with a stream of hidden watermarked bits [12]. The authors also propose a scheme called "Securing Matrix Counting-Based Secret Sharing," which integrates cryptography and steganography. In traditional secret sharing, a key is shared between authorized parties' participants, with only specific groups required to reconstruct the original key. This approach has gained prominence in securing cryptographic and steganographic data, achieving notable results when combined. The focus is on two specific secret sharing techniques: count-based secret

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

sharing and array-based secret, the latter being an extension of the former. These methods are highlighted for their simplicity and intuitive nature [13].

PRELIMINARIES

Blockchain

Blockchain is a storage system characterized by immutability, decentralization, traceability and verifiability, secure transactions without the need for a trusted third party. Confirmation, decision, interfaces, P2P networks and secure hash protocols, digital signatures, asymmetric encryption, short hashes how and when to create a safe environment for business or transaction [14]. In this decentralized system, transaction records are stored across the blockchain network's nodes. Unlike traditional banking, blockchain eliminates the need for a central authority, relying instead on consensus mechanisms to maintain network operations. These mechanisms address challenges like the Byzantine Generals Problem and double spending by validating transactions and preventing fraud. The consensus ensures the stability, security, and consistency of the network, maintaining integrity across all nodes.

Smart Contract

In 1994, cryptography expert Szabo introduced the concept of smart contracts, although they were not implemented until blockchain technology emerged [15]. Bitcoin's scripting system laid the groundwork for smart contracts, but their functionality was limited due to the non-Turing-complete nature of the original design. Ethereum, however, advanced the use of smart contracts by enabling more complex, self-executing contracts. These contracts automatically execute when predefined conditions are met, allowing transactions to occur without the need for a trusted intermediary. Transactions are then permanently recorded in an open, transparent, and immutable manner, ensuring their verifiability. Unlike traditional contracts, smart contracts are end-to-end and users are freed from brokerage commissions and cumbersome processes.

Ethereum

The Ethereum block-chain is a public platform for creating and enforcing smart contracts. In Ethereum Virtual Machine (EVM), every node in the Ethereum network relies on the EVM to ensure that the network runs continuously. The EVM handles tasks such as managing gas fees and user account data, including addresses and balances [16]. Smart contracts, once designed and compiled using Solidity, are deployed on the EVM in Byte-code form. Unlike Bitcoin's scripting system, the EVM is Turing-complete, allowing for more complex operations. Running a program on the EVM requires gas fees, and if the gas is insufficient, the program halts automatically, preventing it from running indefinitely. This feature helps reduce this fixes an issue that could prevent malware from being removed.

Interplanetary File System

Interplanetary File System (IPFS) is a protocol and database system designed to store data transfer. It integrates modules like Default Dependency Table (DHT), Git version control, and self-monitoring, system File System (SFS) allows files to be stored in a traceable system and the process is irreversible and cannot be repeated. Prior to IPFS, block-chain-based applications struggled with large file storage, as it was costly and inefficient to store files directly on block-chains [17]. Centralized servers were often used, but these are vulnerable to hacking and file deletion. IPFS solves these issues by offering permanent, undetectable storage.

PROPOSED WORK

Centralized System

In a centralized approach, the data owner uploads the data to a central server and users have access to it. However, the main problem is that cloud providers can be very unreliable.. They are vulnerable to both external attacks and internal threats from malicious employees, raising significant data security issues. For instance, employees at companies like Amazon may leak sensitive information for personal gain, and cloud providers might eavesdrop on users' private data. To mitigate these risks, cryptography access control techniques are used, encrypting data with a secret key that can only be decrypted by those with the correct key. However, this model requires all users to trust a single authority, which can lead to a single point of failure. In fact, key stakeholders are often divided into multiple areas or trust organizations. The central authority serves as the main server, where the data owner uploads their files, while domain au-

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

thorities are responsible for specific partitions of the server and the users within their domains. Two primary issues in centralized systems are internal data manipulation and the risk of a single point of failure.

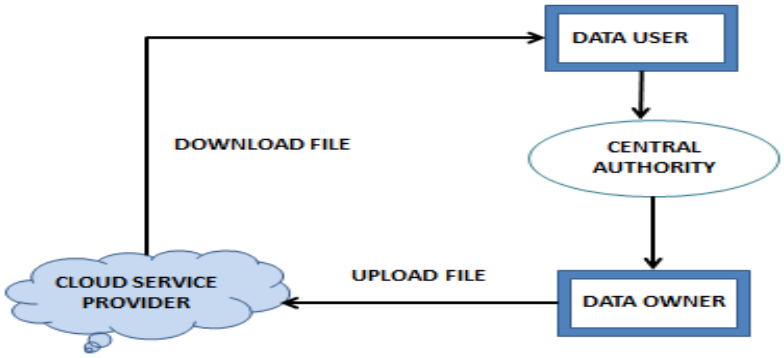

Figure 1: Centralized system Process

IPFS based decentralized system

A decentralized system leveraging block-chain technology is designed to overcome issues like single authority failure, internal data manipulation, excessive processing on the consumer end, and communication overhead. Block-chain enables transparent tracking of data access logs, facilitating audit able and secure access control. This study proposes a robust and efficient method for data transfer through a block chain-based decentralized framework. The IPFS protocol is utilized to establish the decentralized block-chain infrastructure. Files are uploaded to a cloud server by the data owner, after which the block-chain generates a cryptography hash value using the SHA256 key management technique. This hash value is distributed across the network to authorized users. Users with the necessary access rights can retrieve both the hash value and the original file content. In a decentralized network, the original data cannot be manipulated by any user since any alteration triggers the creation of a new hash code, ensuring data integrity. This model enhances security compared to centralized systems. Additionally, the decentralized system eliminates the single point of failure issue, as block-chain functions like a distributed system, where every node keeps a copy of data from other nodes, ensuring easy data recovery in case of failure.

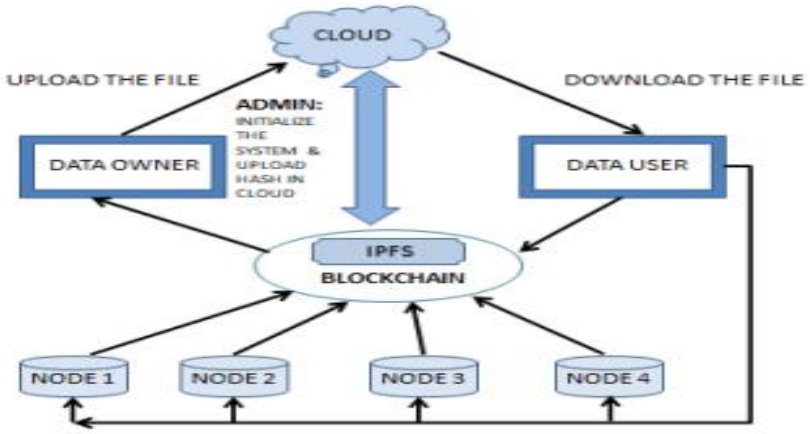

Figure 2: Decentralized system using IPFS

In figure 2, this comprises six distinct entities. To facilitate understanding of the subsequent theoretical algorithms, the syntax of the procedural flow is also outlined.

Administrator: Responsible for configuring system parameters and initializing the system.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Domain Authority (DA): Manages user credentials within its domain via IPFS. Each DA oversees multiple users in a specific domain.

Cloud Service Provider (CSP): Provides storage solutions for data owners.

Data Owner (DO): Since CSP is not fully trustworthy, the DO encrypts files to control data access. The DO creates access policies, encrypts files before uploading them to the cloud, and separately uploads the key and data cipher-text to IPFS.

IPFS: The system acts as a foundational backbone for all entities, generating distinct hash codes for the data and key cipher-text uploaded by the data owner (DO). To maintain integrity and ensure immutability, IPFS is utilized to store public parameters and access metadata securely. Additionally, it facilitates partially trusted computing for business operations and enables collaborative management of user credentials by multiple designated authorities (DAs).

RESULT & DATA ANALYSIS

This section evaluates the security and performance of the proposed block chain-based decentralized data exchange system, demonstrating its reliability in a not-fully-trusted cloud environment.This work addresses the issue of a single point of failure by using a semi-decentralized block-chain approach, where domain authorities assign user keys instead of a central authority. Security is enhanced through block-chain'saudit- able properties, ensuring confidentiality even if a cloud server is compromised. The system resists collusion attacks by binding decryption to specific users, preventing malicious collaboration. User authentication is secured through audit- able access logs on the block-chain, allowing transparent and trustworthy enforcement of access policies. IPFS ensures transaction privacy and protects sensitive data by integrating block chain-based permission control.

Table 1. Processing of Time of User

Number of user	Time(ms)
1000	1.1
2000	2.2
3000	5
4000	7
5000	8

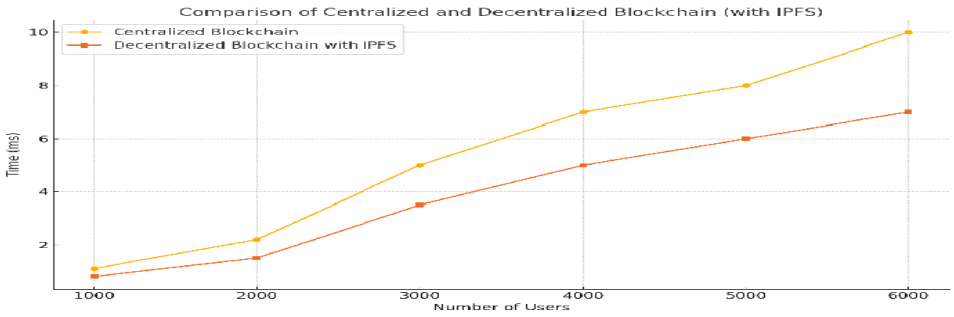

Figure 3: Comparison of centralized system and decentralized block-chain with IPFC

Figure 3. shows, a centralized block-chain system, the time increases sharply as the number of users grows, pointing to significant scalability issues. For 6,000 users, the time reaches 10 ms, highlighting the system's struggle to handle higher loads effectively. In contrast, a decentralized block-chain system utilizing IPFS experiences a slower increase in time as the number of users grows. Despite the load, it remains more efficient, with a maximum time of 7 ms for 6,000 users, showcasing better scalability and handling of larger user bases.

CONCLUSION

The graph highlights the superior scalability and efficiency of decentralized block-chain systems integrated with IPFS compared to centralized block-chains. While both systems experience increased time with higher user loads, the de-

centralized approach demonstrates better performance, making it more suitable for scenarios requiring high scalability and data integrity. IPFS contributes to reducing latency by efficiently managing data distribution and retrieval.The proposed block chain-based decentralized system addresses key issues of centralized systems, such as single points of failure and data manipulation, by integrating distributed IPFS technology. Decentralized access control ensures secure and low-cost file access, with immutable data integrity maintained through block-chain's hashing mechanism. Additionally, the system resists malicious users and unreliable cloud servers, offering enhanced security and reliability over centralized approaches.

REFERENCES

[1] LNCS Homepage, http://www.springer.com/lncs, last accessed 2016/11/21. Kumari Poonam, Singh Meeta.: Cloud Security and Challenges. Review Of International Geographical Education ISSN: 2146-0353 ● © RIGEO ● 11(8), SPRING (2021).
[2] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., Rimba, P.: A taxonomy of blockchain-based systems for architecture design. IEEE international conference on software architecture (ICSA). IEEE, 243-252 (2017).
[3] Hao, J., Huang, C., Ni, J., Rong, H., Xian, M., Shen, X.S.: Fine-grained data access control with attribute-hiding policy for cloud-based IoT. Comput. Netw. 153, 1–10 (2019).
[4] Kumari Poonam, Singh Meeta.: A Review: Different Challenges in Energy – Efficient Cloud Security. IOP Conf. Series: Earth and Environmental Science **785** 012002 IOP Publishing. doi:10.1088/1755-1315/785/1/012002 (2021).
[5] Lyu, Q., Qi, Y., Zhang, X., Liu, H., Wang, Q., Zheng, N.: SBAC: A secure blockchain-based access control framework for information-centric networking. J. Netw. Comput. Appl. 149, 102444 (2020).
[6] Gai, K., Guo, J., Zhu, L., Yu, S.: Blockchain meets cloud computing: A survey. IEEE Commun. Surv. Tutorials 22, 2009–2030 (2020)
[7] Dalal, J., Chaturvedi, M., Gandre, H. and Thombare, S.: Verification of Identity and Educational Certificates of Students Using Biometric and Blockchain. Available at SSRN 3564638 (2020).
[8] Wang, Z., Lin, J., Cai, Q., Wang, Q., Zha, D. and Jing, J.: Blockchain-based certificate transparency and revocation transparency. IEEE Transactions on Dependable and Secure Computing (2020).
[9] Praveen. M. Dhulavvagol*, S G Totad, Mahadev Rashinkar, Ribhav Ostwal, Suprita Patil, Priyanka M Hadapad.: Scalable Blockchain Architecture using off-chain IPFS for Marks Card Validation. Procedia Computer Science 215 p. 370–379 (2022).
[10] Baldi, M., Chiaraluce, F., Frontoni, E., Gottardi, G., Sciarroni, D. and Spalazzi, L.: Certificate Validation Through Public Ledgers and Blockchains. In ITASEC pp. 156-165 (2017).
[11] Gutub, A.: Watermarking Images via Counting-Based Secret Sharing for Lightweight Semi- Complete Authentication. International Journal of Information Security and Privacy (IJISP), 16(1), 1-18. http://doi.org/10.4018/IJISP.2022010118 (2022).
[12] Almehmadi, E., Gutub, A.: Novel arabic e-text watermarking supporting partial dishonesty based on counting-based secret sharing" Arab. J. Sci. Eng. https://doi.org/10.1007/s13369-021-06200-7b (2021).
[13] Al-Shaarani, F., Gutub, A.: Securing matrix counting-based secret-sharing involving crypto steganography. J. King Saud Univ. – Comput. Inf. Sci. https://doi.org/10.1016/j.jksuci.2021.09.009 (2021).
[14] Kumari Poonam, Singh Meeta.: Blockchain-Based Distributed Data Security and trust management System for Cloud Computing. Library Progress International| Vol.44 No.3 | P. 25576-25593 (2024).
[15] Smita Athanere, Ramesh Thakur. Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing. Journal of King Saud University – Computer and Information Sciences 34 pp. 1523–1534, https://doi.org/10.1016/j.jksuci.2022.01.019 (2022).
[16] Gajala Praveen 1*, Piyush Kumar Singh 2 and Prabhat Ranjan.: A Blockchain Integrated IPFS-based System. International Journal of Intelligent Systems and Applications in Engineering IJISAE, 12(13s), 288–301 (2024).
[17] Nishara Nizamuddin, Haya R. Hasan, Khaled Salah. IPFS-Blockchain-based Authenticity of OnlinePublications. Chapter *in* Lecture Notes in Computer Science · DOI: 10.1007/978-3-319-94478-4_14 (2018).