



International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)



Research Paper**A Decentralized Cloud Storage Security Framework Based on IPFS and Ethereum Integration**J. Sravanthi¹, Pinninti Abhinav², Poosa Nagaraju², Pulla Nikhitha², Thota Naga Jyothi²¹Assistant Professor, ²UG Student, ^{1,2}Department of Computer Science and Engineering (Data Science)^{1,2}Vaagdevi College of Engineering (UGC-Autonomous), Bollikunta, Warangal, 506005, Telangana**Abstract**

The rapid evolution of cloud computing has revolutionized digital data storage and sharing, enabling users to access information anytime and anywhere. Despite these advantages, cloud-based systems face major challenges related to data security, privacy protection, and trust management, particularly when handling sensitive user information. Conventional cloud storage solutions operate on centralized architectures, where a single cloud service provider manages and controls the stored data. This centralized model introduces significant risks, including single points of failure, unauthorized data access, data manipulation, and limited visibility into data-sharing activities. In many traditional systems, data protection mechanisms rely on basic encryption methods without strong auditing or verification features, leaving them vulnerable to insider attacks and external cyber threats. Furthermore, the absence of immutable transaction records and robust key management practices reduces accountability and weakens user confidence in cloud environments. To address these shortcomings, the proposed system presents a secure cloud data sharing framework that combines Elliptic Curve Cryptography (ECC) with blockchain technology. In this approach, user files are encrypted using ECC before being uploaded to the cloud, ensuring strong data confidentiality and protection against unauthorized access. Simultaneously, blockchain technology is employed to record file metadata and transaction details in a decentralized and tamper-resistant ledger, enabling transparent and verifiable audit trails. The decentralized architecture eliminates reliance on a single authority, enhances trust, and prevents unauthorized modification of stored records. Additionally, secure authentication and controlled access mechanisms further reinforce system security. By integrating advanced cryptographic encryption with decentralized verification, the proposed solution enhances data integrity, improves transparency, and establishes a reliable and accountable framework for secure cloud data sharing.

Keywords: Cloud Data Security, Blockchain Technology, Elliptic Curve Cryptography (ECC), Decentralized Data Sharing, Access Control, Cryptographic Security.

Received: 06-02-2026

Accepted: 13-03-2026

Published: 20-03-2026

1. Introduction

In our increasingly digital world, the integration of blockchain technology and cloud computing has emerged as a promising innovation to address the challenges of data

storage. As the volume of data continues to grow exponentially, securely storing, managing, and retrieving large files has become a critical issue. Blockchain technology, renowned for its decentralized and immutable ledger, provides a robust

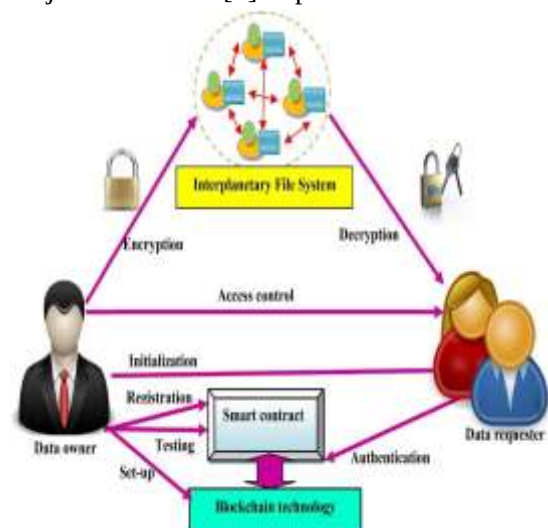
framework for securing sensitive health information. By encrypting data and recording transactions in a tamper-proof manner, blockchain ensures data integrity, authenticity, and auditability, thereby mitigating the risk of unauthorized access, fraud, and data manipulation. The issue with this method is data security. As a result, a trusted computer system utilizes hardware and software assurance methods to process several classified or sensitive data levels. This system satisfies the specified dependability and security criteria. Unfortunately, despite the numerous benefits of the cloud in ensuring the confidentiality, integrity, and availability of stored data, the number of security breaches is continuously rising. Even the advent of cloud technology comes with several different risks for organizations, particularly in secure computing. To preserve privacy and security of data, it is usually stored on the cloud server in the form of ciphertext. When a user requests access to encrypted data, a third-party access key is required. The system's security will be affected if the third party is untrustworthy.

Fig. 1: Blockchain-enabled framework for secure data access control.

To solve this problem, we may use a decentralized system using Blockchain to create a multi-authority-based access control scheme for data sharing. Blockchain technology is characterized by decentralization, openness, autonomy, and independence from a trusted third party. It makes use of encryption technology to preserve anonymity, and it is generally safer than standard data storing methods. A lot of promise exists when blockchain technology is combined with cloud data sharing systems. Currently, blockchain technology may be utilized to address issues such as secure data access via a decentralized multi-authority framework.

2. Literature Survey

Routh et al. [1] analyzed three traditional and seven hybrid cloud computing access control systems, emphasizing the relevance of granularity in model selection and demonstrating the benefits of fine-grained access control mechanisms. Patil et al. [2] investigated many blockchain-based techniques that have been suggested in the literature to manage IoT device access and enhance privacy and security in the supply chain, vehicular ad hoc network, and healthcare networks. Butun et al. [3] examined peer-to-peer (P2P) network access control schemes and proposed a threshold signature-based authentication system, trusted computing and reputation-based authorization systems, and Certificate Revocation List (CRL) with group signatures to revoke permission from blockchain systems. Wijesekara et al. [4] explored the blockchain-



based access control in networking to ensure that only authorized devices complete defined operations to prevent malicious activity. The author classifies various access control techniques into four proposals and evaluates them based on blockchain roles, access control methodologies, network aspects, and other criteria. Sharma et al. [5] proposed blockchain technology to secure cloud storage, motivated by the increasing demand and importance of blockchain innovation in addressing recent technological issues. Praharaj et al. [6] reviewed the literature to identify and evaluate cloud access control requirements and

techniques, answering research questions on security models, proposed mechanisms, and their pros and cons to help researchers and practitioners evaluate existing models and identify gaps. Li et al. [7] offered a cloud-edge hybrid trust management framework with a double-blockchain transaction model. They also provided a taxonomy and evaluation of blockchain-based trust management techniques in cloud computing, as well as analysed and compared them. They also made suggestions for future research and problems. Our systematic review examines how blockchain technology can improve cloud access control.

Rezaei et al. [8] provided a novel way to decentralize authentication, authorization, and auditing responsibilities through the utilization of blockchain technology. The transparent blockchain preserves auditing data, preventing impersonation, collusion, and manipulation. The performance analysis highlights the solution's efficient transaction-related computations. Ri et al. [9] introduced a blockchain-based Role-Based Access Control (RBAC) architecture with Separation of Duties (SoD) constraints and a cloud-based access control system. The proposed access control approach confirms role ownership using a user-generated keypair of private and public keys and manages access requests through their model. An Ali cloud environment simulation shows that the approach improves security and access control by integrating Separation of Duties (SoD) requirements on the blockchain. Mohammadpayam Almasian et al. [10] proposed a blockchain-based cloud storage access control architecture for fast revocation. The architecture uses public blockchain and cloud service models to solve storage, accessibility, and backup issues for businesses without a trusted element. The blockchain connection allows financial transaction outsourcing and denial-of-service protection. Public blockchain systems with smart contracts may improve web application security and service. Smart contracts prevent

centralization and single points of failure in access control frameworks, unlike conventional methods that may be insecure and difficult to maintain.

3. Proposed Methodology

The rapid digital transformation and increasing reliance on cloud storage systems have amplified the importance of data security, transparency, and integrity. Traditional cloud architectures, while efficient in providing large-scale storage and accessibility, suffer from centralized control, making them prone to security breaches, unauthorized access, and single points of failure. To address these limitations, this project introduces a hybrid IPFS-Ethereum framework for decentralized cloud storage security, which leverages the combined strengths of the IPFS and Ethereum blockchain technologies to establish a secure, transparent, and tamper-proof cloud storage environment.

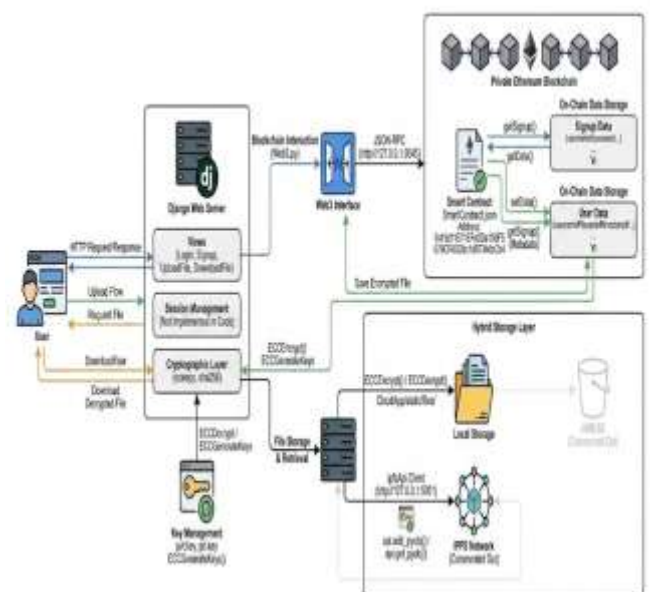


Fig. 2: System architecture of cloud storage security.

In this framework, IPFS serves as the decentralized file storage layer, where data is divided into smaller chunks, distributed across multiple nodes, and identified by unique cryptographic hash values. This ensures

redundancy, scalability, and resistance to data loss or manipulation. Unlike conventional centralized storage, where all data resides in one location, IPFS ensures that no single entity has full control over the data, thereby enhancing data availability and resilience. At the same time, the Ethereum blockchain plays a crucial role in managing transaction verification and access control. Each file upload, download, or modification is recorded as an immutable transaction on the blockchain, guaranteeing transparency and traceability across all operations.

Elliptic Curve Cryptography (ECC)

The Elliptic Curve Cryptography technique serves as the backbone of data security in this project. It provides a powerful yet lightweight encryption method to protect files before they are uploaded to the IPFS network and ensures that only authorized users can decrypt them later. ECC works on the mathematical principles of elliptic curves over finite fields, allowing strong encryption with smaller key sizes compared to traditional algorithms like RSA. In this project, ECC is responsible for generating unique key pairs for each user: a public key for encryption and a private key for decryption. Before any file is stored on IPFS, it is encrypted using the user's public key, ensuring confidentiality even in a distributed environment. When a file needs to be retrieved, the user's private key is used to decrypt it back into its original form. This cryptographic approach ensures end-to-end security, data authenticity, and user-specific access control across the decentralized storage framework.

Key Generation Process: The ECC system begins by generating a pair of cryptographic keys: one public and one private. The private key is a randomly selected large number, while the public key is derived mathematically from it using an elliptic curve function. These keys are unique to each user and form the basis for secure encryption and decryption processes.

Private Key Storage and Protection: Once generated, the private key is securely stored on the user's local machine or within the Django framework's encrypted storage. This key is never transmitted or shared over the network to avoid unauthorized access. It acts as the ultimate decryption key that enables users to unlock their encrypted files safely.

Public Key Distribution: The public key, unlike the private key, can be freely shared within the system. It is stored in the blockchain-based user record during registration for verification and encryption purposes. When other entities or the system needs to encrypt data for that user, they use the associated public key.

File Encryption Using Public Key: Before a file is uploaded to IPFS, it is first encrypted using the user's public key. This converts the plain data into an unreadable cipher format that only the corresponding private key can decrypt. Even if the encrypted file is accessed on the IPFS network, it remains useless to unauthorized users.

Encryption Process Implementation: The encryption process uses an ECC function that transforms the file data into a series of encrypted points on the elliptic curve. Each byte or data block is mathematically mapped using the public key curve parameters. This ensures that the encrypted data cannot be reversed without the private key's knowledge.

Data Transmission to IPFS: Once the encryption is complete, the encrypted file is transmitted to the IPFS network for decentralized storage. Even during transmission, the encrypted nature of the file ensures it cannot be intercepted or tampered with. This maintains data confidentiality throughout the file's journey to distributed nodes.

File Retrieval and Ciphertext Access: When the user requests to download a file, the system retrieves the encrypted version from IPFS. The file remains in cipher form during the entire retrieval process, preventing

unauthorized reading. This ensures that even if intermediate network nodes access the data, they cannot interpret it.

File Decryption Using Private Key: The user's private key is used to decrypt the encrypted data back into its original readable form. The decryption process mathematically reverses the elliptic curve operations applied during encryption. This restores the file exactly as it was before encryption, ensuring accuracy and data integrity.

Data Integrity Verification: After decryption, the system verifies the file's integrity using its hash value stored in the blockchain. If the computed hash matches the stored one, it confirms that the file has not been altered or corrupted. This step guarantees authenticity and reinforces trust in the entire data handling process.

4. Results and Discussion

Results section presents the functional outcomes of the proposed Hybrid IPFS–Ethereum decentralized cloud storage system, focusing on the user interaction flow from initial access to secure file storage and retrieval. Each interface screen highlights key stages in system operation, emphasizing usability, security, and integration of decentralized technologies. The discussion illustrates how authentication, cryptographic file handling, and distributed storage ensure controlled access, data integrity, and confidentiality, providing a practical view of the system's secure and verifiable cloud storage capabilities.



Fig. 3: User sign up.

Fig. 3 depicts the user signup screen used for registering new users into the decentralized cloud storage system. This interface allows users to submit personal and authentication-related details required for account creation. The signup process ensures controlled access to the system by validating user information before registration. Successful registration enables users to securely interact with storage and retrieval functionalities. This screen plays a critical role in establishing authenticated identities within the decentralized environment. Fig. 4 illustrates the user login screen that enables registered users to authenticate themselves within the system. It verifies user credentials before granting access to protected functionalities such as file upload and download. The login process ensures that only authorized users can interact with encrypted data and decentralized storage services. This screen acts as a security checkpoint for enforcing access control. It represents the transition from public access to authenticated system usage.

[Upload File to Cloud](#)
[Access/Retrieve Cloud](#)
[Logout](#)

Data Owner	IPFS File Address	Upload Date/Time	Filename	Download File
Intelligence IV CSE-C FINAL TITLES 01-12-2020.xlsx	2020-01-17 12:38:08	IV CSE-C FINAL TITLES 01-12-2020.xlsx	Download File	
Intelligence Requirements 01.xls	2020-01-17 12:50:38	Requirements 01.xls	Download File	

Fig. 5 presents the file upload interface used to securely store data in the decentralized cloud environment. This screen allows authenticated

5. Conclusion

References

- [1] Routh, Aman & Ranjan, Prabhat. (2024). A Comprehensive Review on Granularity Perspective of the Access Control Models in Cloud Computing. 1-

6.
10.1109/IATMSI60426.2024.10503154.
- [2] B. Patil, Pradnya & Manoharan, Sangeetha & Bhaskar, Vidhyacharan. (2021). Blockchain for IoT Access Control, Security and Privacy: A Review. *Wireless Personal Communications*. 117. 1-20. 10.1007/s11277-020-07947-2.
- [3] Butun, Ismail & Österberg, Patrik. (2020). A Review of Distributed Access Control for Blockchain Systems Towards Securing the Internet of Things. *IEEE Access*. 9. 5428-5441. 10.1109/ACCESS.2020.3047902.
- [4] Wijesekara, Patikiri Arachchige Don Shehan. (2024). A Literature Review on Access Control in Networking Employing Blockchain. *Indonesian Journal of Computer Science*. 13. 10.33022/ijcs.v13i1.3764.
- [5] Sharma, Pratima & Jindal, Rajni & Borah, Malaya. (2020). Blockchain Technology for Cloud Storage: A Systematic Literature Review. *ACM Computing Surveys*. 53. 10.1145/3403954.
- [6] Praharaj, Lopamudra & Gupta, Maanak. (2023). A Systematic Review of Access Control in Cloud Computing. 10.1201/9781003287612-3.
- [7] Li, W., Wu, J., Cao, J. *et al.* Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. *J Cloud Comp* 10, 35 (2021). <https://doi.org/10.1186/s13677-021-00247-5>
- [8] Rezaei, Adib & Mirsian, Sina. (2025). Leveraging Blockchain Technology for Secure Authentication, Auditing, and Access Control: A Review.
- [9] Mahesh Ganji. (2025). Enhancing Oracle Cloud HR Reporting Through AI-Driven Automation. *Journal of Science & Technology*, 10(6), 28–36. <https://doi.org/10.46243/jst.2025.v10.i06.pp28-36>
- [10] Saikumar, B. (2023). Enhancing Client Engagement through AI-Driven Real-Time Reporting and Automated Alerts. *International Journal of Enhanced Research in Science, Technology & Engineering*, 12(11), 111–117. <https://doi.org/10.55948/ijerste.2023.1115>
- [11] Ri, Ok-Chol & Kim, Yong-Jin & Jong, You-Jin. (2022). Blockchain-based RBAC Model with Separation of Duties constraint in Cloud Environment. 10.48550/arXiv.2203.00351.
- [12] Mohammadpayam Almasian, Alireza Shafieinejad, Secure cloud file sharing scheme using blockchain and attribute-based encryption, *Computer Standards & Interfaces*, Volume 87, 2024, 103745, ISSN 0920-5489, <https://doi.org/10.1016/j.csi.2023.103745>