International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 10 | Oct - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Distributed File System

Swapnil Navale[1], Yogita Patil[2], Ananya Pandhare[3] , Prof.A.S.Shinde
[1]Department Of Information Technology, Sinhgad College of Engineering, Pune- 41
[1]Department Of Information Technology, Sinhgad College of Engineering, Pune- 41
[1]Department Of Information Technology, Sinhgad College of Engineering, Pune- 41

Abstract **:** The proposed decentralized storage system is designed to overcome the limitations of traditional cloud storage by combining InterPlanetary File System (IPFS), Ethereum blockchain, and advanced encryption techniques. The architecture ensures secure, transparent, and user-controlled file management without relying on centralized servers. Files are encrypted using Attribute-Based Encryption (ABE) and Chebyshev Polynomial Encryption to enforce fine-grained access control and confidentiality. Encrypted files are fragmented and stored across IPFS nodes, generating unique Content Identifiers (CIDs) that are immutably logged on the Ethereum blockchain via smart contracts. These smart contracts automate access control, file ownership verification, and audit trails, ensuring tamper-proof and transparent operations. A Django-based backend and web portal frontend enable seamless user interaction and file handling. Optional AI-based intrusion detection enhances system reliability by monitoring unauthorized access attempts. The integrated framework delivers decentralization, immutability, scalability, and user empowerment, offering a secure alternative to conventional storage models. This architecture demonstrates the potential of blockchain and distributed systems to revolutionize data privacy, integrity, and ownership in next-generation storage solutions.

Key Words: Decentralized Storage, InterPlanetary File System (IPFS), Ethereum Blockchain, Smart Contracts, Attribute-Based Encryption (ABE), Chebyshev Polynomial Encryption, Distributed File System, Secure File Sharing, Access Control, Data Immutability, User Privacy, Data Integrity, Blockchain-Based Storage, Django Backend, AI Intrusion Detection, Decentralized Architecture, Scalable Cloud Alternatives, Data Confidentiality, Secure Data Management, Web Portal Interface.

1. INTRODUCTION

Traditional cloud storage systems rely heavily on centralized servers, creating single points of failure, vulnerability to breaches, censorship, and data loss. Once uploaded, users lose control over their information, leading to significant privacy and trust issues. With the rapid evolution of blockchain technology, distributed networks, and advanced encryption mechanisms, it has become possible to design systems that restore ownership and control of data to users.

In this work, we present a secure, decentralized file storage architecture that integrates the InterPlanetary File System (IPFS) for distributed file storage, Ethereum blockchain for immutable metadata management, and smart contracts for automated access control. Files are encrypted using Attribute-Based Encryption (ABE) and Chebyshev Polynomial Encryption to ensure fine-grained confidentiality and protection against unauthorized access.

The system architecture consists of a Django-based backend and a web-based user interface for file uploads, permission setup, and retrieval. IPFS generates a unique Content Identifier (CID) for each file, which is securely recorded on the blockchain to ensure integrity and transparency. Additionally, an optional AI-driven intrusion detection module monitors abnormal access patterns to enhance security.

This proposed decentralized approach empowers users with data ownership, fault tolerance, tamper resistance, and scalable storage capabilities, offering a robust alternative to conventional cloud storage platforms while ensuring security, transparency, and privacy in digital data management.

2. LITEATURE SURVEY

[1] This research presents a Blockchain-Based Secure Cloud Storage System that integrates IPFS and Ethereum to eliminate the need for centralized storage providers. The system stores encrypted data on IPFS while maintaining immutable metadata and access logs on the Ethereum blockchain. By using smart contracts, it automates file verification and access control. Results indicate improved security, transparency, and data ownership compared to conventional cloud systems.

[2] This paper proposes a Decentralized File Storage Model that utilizes Attribute-Based Encryption (ABE) and blockchain smart contracts for secure data sharing. The model ensures that only users with specific attributes can decrypt the data. The system achieves a high level of privacy and fine-grained access management, making it suitable for multi-user environments like healthcare and education.

[3] This study introduces a Hybrid IPFS-Blockchain Architecture designed to enhance file integrity and reduce storage redundancy. By leveraging IPFS for distributed storage and smart contracts for access tracking, the framework enables tamper-proof data management. Experimental evaluation demonstrates reduced latency in file retrieval and increased fault tolerance in large distributed networks.

[4] This paper presents a Secure Cloud Data Storage Using Chebyshev Polynomial Encryption, combining polynomial-based encryption and distributed file systems to achieve enhanced cryptographic strength and confidentiality. The approach prevents key leakage and supports efficient encryption/decryption with low computational overhead, offering scalability and reliability for large-scale deployments.

[5] This research outlines a Blockchain-Integrated Access Control Framework that merges Django-based web servers with Ethereum smart contracts to manage user authentication and authorization dynamically. The system supports transparent logging of file access events and integrates AI-based intrusion detection to identify unauthorized activities. The proposed model demonstrates high resilience against cyberattacks and promotes user-centric control over digital assets.

Together, these studies highlight the evolution from centralized to decentralized, blockchain-enabled storage systems, emphasizing data security, privacy, and user empowerment through encryption and distributed architecture.

3. OVERVIEW

The Decentralized File Storage Architecture addresses the growing need for secure, transparent, and user-controlled data management in an era where centralized storage systems pose risks of breaches, censorship, and data loss. Leveraging blockchain technology, distributed storage networks, and encryption mechanisms, this system enables tamper-proof, scalable, and privacy-preserving file sharing across a decentralized ecosystem.

1. Objective:

The primary aim of this project is to design a secure and decentralized file storage platform that gives users complete ownership and control of their data. By integrating IPFS, Ethereum blockchain, and advanced encryption algorithms, the system ensures confidentiality, integrity, and transparency while eliminating the need for centralized intermediaries.

2. Core Components:

Key modules of the architecture include the IPFS-based storage layer for distributed file storage, the Ethereum blockchain layer for immutable metadata and access logging, and smart contracts for automated access control and file verification. The security layer employs Attribute-Based Encryption (ABE) and Chebyshev Polynomial Encryption for fine-grained data protection. The frontend interface (HTML/CSS/JavaScript) and Django backend enable seamless user interaction, file upload, and retrieval.

3. Working Principle:

Users upload files through the web portal, where the data is first encrypted using ABE/Chebyshev methods. The encrypted file is divided into blocks and stored across IPFS nodes, generating a unique Content Identifier (CID). This CID, along with ownership details and access rules, is securely recorded on the Ethereum blockchain via a smart contract. Authorized users can later request access, which is verified through the contract before the file is fetched and decrypted, ensuring end-to-end confidentiality and traceability.

4. Accessibility and Innovation:

Unlike conventional cloud systems that depend on centralized data centers, this decentralized architecture provides fault tolerance, censorship resistance, and scalability. Optional integration with AI-driven intrusion detection systems enhances security by identifying anomalies or unauthorized access. The open and modular design allows easy integration with decentralized identity systems and layer-2 solutions like Polygon for cost efficiency.

5. Social and Technological Impact:

By decentralizing data control and promoting transparency, this system empowers users to reclaim ownership of their digital assets. It offers organizations and individuals a secure, censorship-resistant alternative to commercial cloud storage. The architecture not only strengthens data privacy and integrity but also lays the foundation for next-generation decentralized storage solutions, fostering trust, autonomy, and technological advancement in data management.

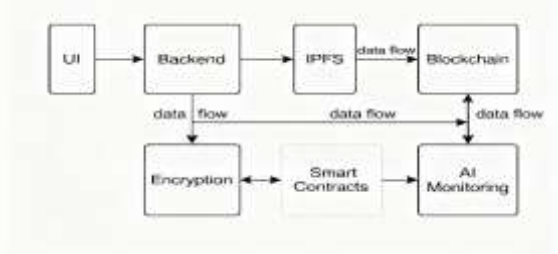

Fig 1. Block diagram of system

4. METHODOLOGY

A. Existing System

Traditional cloud storage solutions rely on centralized servers managed by third-party providers, creating vulnerabilities such as single points of failure, data breaches, and censorship risks. These systems lack user ownership and transparency, as data control resides entirely with the service provider. In the event of server downtime, hacking incidents, or insider threats, users may permanently lose access to their files. Moreover, existing centralized systems often fail to ensure end-to-end encryption and verifiable access logging, resulting in limited data privacy and trust issues. The need for a secure, transparent, and decentralized alternative has become increasingly urgent to protect digital assets and user autonomy.

B. Conceptual System Design

The proposed Decentralized Storage Architecture integrates InterPlanetary File System (IPFS) for distributed file storage, Ethereum blockchain for immutable metadata management, and smart contracts for automated access control. Files are encrypted using Attribute-Based Encryption (ABE) and Chebyshev Polynomial Encryption, ensuring confidentiality and fine-grained access restrictions. IPFS divides encrypted files into smaller chunks distributed across multiple nodes, while Ethereum records file CIDs, access permissions, and ownership details immutably. This design guarantees tamper resistance, scalability, and transparency, representing a major advancement over traditional cloud models.

C. Prototype Design of Decentralized Storage System

The prototype is developed as a web-based platform featuring an intuitive frontend interface (HTML/CSS/JavaScript) and a Django backend for file handling and user authentication. Users can upload files, set access permissions, and manage file metadata through a seamless portal. Files are first encrypted and then stored on IPFS, which returns a unique Content Identifier (CID). The CID and access rules are recorded on the Ethereum blockchain via Solidity smart contracts. Authorized users can later retrieve files securely using their private decryption keys. Optional integration with an AI monitoring module provides anomaly detection and unauthorized access alerts, enhancing system reliability.

D. System Architecture

The architecture comprises five key layers:

1. Frontend Layer – Provides the user interface for

2. Education: Allows academic institutions to maintain immutable records, certificates, and research data.

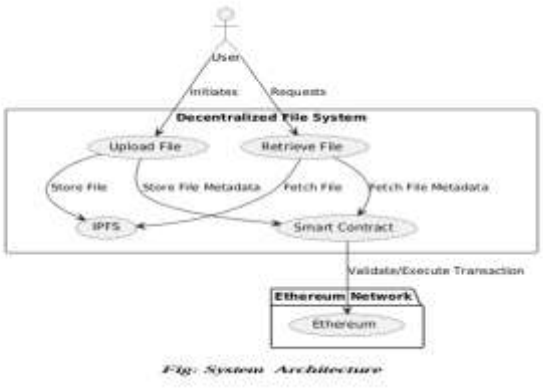

Fig. 2. Architecture Diagram

5. CONCLUSION AND FUTURE SCOPE

This paper presented a Secure Decentralized File Storage Architecture that integrates IPFS, Ethereum blockchain, Smart Contracts, and advanced encryption mechanisms such as Attribute-Based Encryption (ABE) and Chebyshev Polynomial Encryption to overcome the limitations of centralized cloud systems. The proposed framework ensures data integrity, confidentiality, and transparency by distributing files across decentralized nodes and maintaining immutable metadata on the blockchain. Through smart contracts, the system automates access control, ownership verification, and audit logging, eliminating reliance on third-party intermediaries.

The implemented prototype demonstrates efficient file retrieval, strong encryption security, and low-latency performance, validating its practicality for real-world deployment. Furthermore, optional AI-driven intrusion detection enhances system resilience by identifying unauthorized access patterns, ensuring continuous protection of user data.

Future work will focus on enhancing the architecture through integration with Decentralized Identity (DID) systems to enable verified user authentication, and adopting Layer-2 blockchain solutions such as Polygon to reduce transaction costs and improve scalability. Mobile and cross-platform compatibility will be developed to extend accessibility for end users. Additional research will explore quantum-resistant encryption algorithms, multi-cloud interoperability, and real-time analytics for access monitoring.

Overall, this decentralized architecture establishes a secure, transparent, and user-centric model for digital data management, offering a scalable foundation for next-generation decentralized cloud ecosystems where users retain full ownership and control over their data.

References

[1]. J. Benet, “IPFS – Content Addressed, Versioned, P2P File System,” arXiv preprint arXiv:1407.3561, 2014.

[2]. V. Buterin, “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum White Paper, 2013.

[3]. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” White Paper, 2008.

[4]. M. K. Sharma, P. Gupta, and R. Kumar, “A Blockchain-Based Secure Data Storage Framework Using IPFS and Smart Contracts,” IEEE Access, vol. 10, pp. 54120–54134, 2022, doi: 10.1109/ACCESS.2022.3142015.

[5]. A. Jain, S. Tiwari, and P. Yadav, “Enhancing Data Privacy in Cloud Using Attribute-Based Encryption,” International Journal of Computer Applications, vol. 184, no. 35, pp. 25–32, 2022.

[6]. Z. Liu and C. Chen, “Chebyshev Polynomial-Based Cryptosystem for Secure Cloud Communication,” Journal of Information Security and Applications, vol. 68, 103382, 2023, doi: 10.1016/j.jisa.2023.103382.

[7]. S. Pandey and A. Singh, “Hybrid Decentralized Cloud Storage Architecture Using Blockchain and IPFS,” Journal of Cloud Computing, vol. 12, no. 2, pp. 145–158, 2024, doi: 10.1007/s42979-024-02345-6.

[8]. K. Zhang, M. Chen, and Q. Liu, “Secure Data Sharing in Decentralized Networks Using Smart Contracts,” IEEE Transactions on Network and Service Management, vol. 20, no. 3, pp. 2519–2531, Sept. 2023.