International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 2, March-April 2026||

DOI:10.15662/IJRAI.2026.0902008

Decentralized Secure File Storage Platform

S.Yoga, M.Sc(CS&IT)., M.Sc., (Maths)., M.Phil(CS)., M.Phil., (Maths).[1] , M. Jayajothi[2]

Department of Computer Science, Sakthi College of Arts and Science for Women, Oddanchatram, Tamilnadu, India[1]

M. Sc (Computer Science), Department of Computer Science, Sakthi College of Arts and Science for Women, Oddanchatram, Tamilnadu, India[2]

Publication History: 06.02. 2026 (Received); 11.03.2026 (Revised); 15.03. 2026 (Accepted); 18.03.2026 (Published).

ABSTRACT: The introduction starts by pointing out the increasing importance of file sharing and storage in the digital age, with an emphasis on the traditional reliance on centralized systems. Discuss the vulnerabilities and limitations of these systems, such as a single point of failure and susceptibility to security breaches. Then, introduce the concept of decentralization and the role blockchain plays in transforming file sharing and storage. Emphasize the potential of blockchain to address the shortcomings of centralized systems by providing enhanced security, transparency, and trust. This paper focuses on decentralized secure data storage and sharing, high availability of data, and efficient utilization of storage and sharing resources.

KEYWORDS: Decentralized Storage, Blockchain Technology, InterPlanetary File System (IPFS), Distributed Ledger Technology (DLT), Data Security, File Encryption, Peer-to-Peer Networks, Smart Contracts, Data Integrity, Cloud Storage, Access Control, Secure File Sharing

I. INTRODUCTION

In the realm of digital information management, traditional centralized cloud storage systems face escalating concerns over security vulnerabilities and a susceptibility to breaches. While cloud storage remains a primary option for handling extensive datasets, the drawbacks of centralized control have prompted a paradigm shift. Blockchain technology has emerged as a transformative force, introducing decentralized file sharing and storage systems that fundamentally alter the landscape of data management. The essence of this shift lies in moving away from centralized models, where data resides in single points of control, towards a decentralized framework facilitated by blockchain. Inherently securing data, blockchain operates as a distributed ledger technology, establishing a decentralized cloud storage system. This innovation hinges on the formation of a peer-to peer network, allowing any connected computing node to actively engage and optimize resource utilization. A pivotal player in this transformation is the Interplanetary File System (IPFS), a protocol that enhances the security and efficiency of file storage on multiple network peers. In this proposed system, user files undergo encryption and distribution across the IPFS network, with hash values pointing to file paths stored on the blockchain.

II. LITERATURE SURVAY

The reviewed studies focus on decentralized and blockchain-based storage systems, highlighting their evolving role in secure data management. Several research works propose innovative methods such as coding schemes, consensus mechanisms, and smart contract integration to enhance data protection, storage efficiency, and reliability. For instance, blockchain-based secure storage and decentralized networks leverage advanced techniques like double-blockchain structures, vector commitment aggregation, and oracle networks to improve authentication, data integrity, and system performance. Additionally, auditing frameworks and encryption-based architectures have been introduced to ensure transparency, security compliance, and efficient data handling across distributed environments.

Survey and review papers provide insights into decentralized oracle networks, auditing mechanisms, and distributed storage systems, emphasizing their operational frameworks and practical challenges. These studies underline the importance of feature improvements such as compression methods, secure data transfer protocols, and smart contract-based governance to strengthen system architecture. Furthermore, research also explores applications in wireless sensor

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 2, March-April 2026||

DOI:10.15662/IJRAI.2026.0902008

networks and file coin mechanisms, demonstrating how decentralized approaches can support scalable and independent data storage across nodes.

Despite the advancements, several limitations and future research directions have been identified. Common challenges include security loopholes, latency issues, and data transfer speed constraints. Researchers suggest improvements such as integrating artificial intelligence techniques, enhancing consensus algorithms, and optimizing service density to achieve better efficiency and robustness. Moreover, the need for advanced architectures, improved encryption methods, and stronger digital rights management systems is emphasized to address emerging threats and ensure trustworthy decentralized storage solutions.

Overall, the literature indicates that while decentralized and blockchain-based storage systems offer significant advantages in terms of security, transparency, and scalability, further research is required to overcome performance and security challenges. Future developments focusing on hybrid models, AI integration, and optimized protocols are expected to enhance system effectiveness and support broader real-world applications.

III. THEORETICAL BACKGROUND

3.1 PROBLEM IDENTIFICATION

- Traditional file-sharing and storage systems have inherent weaknesses due to their centralized structure, making them susceptible to security breaches, limitations, and system failures. When a centralized system experiences a breakdown, it risks the loss of vital data, and the hefty maintenance costs often result in expensive service charges for users. However, decentralized file sharing and storage systems, operating on Blockchain technology, aim to tackle these challenges by offering a secure, dependable, and transparent platform resilient to failures and malicious attacks. Through Blockchain-based decentralized systems, peer-to-peer interactions facilitate seamless sharing of information, alleviating concerns about potential data loss or system downtime. Moreover, Blockchain technology ensures data security by making each transaction transparent, tamper-proof, and immutable, thereby enhancing trust and reliability in the system.

3.2 PROBLEM SOLVING

- The proposed system for decentralized file storage and sharing prioritizes user control and transparency. Users can access content only with owner permission, while all actions are recorded on the Blockchain, ensuring transparency. Features such as logging, user access control, reputation systems, and hash verification facilitate monitoring and tracking of file-sharing activities. Scalability, performance, and usability are improved through distributed storage (IPFS), optimized smart contracts, user-friendly interfaces, and performance benchmarking. Security and privacy are upheld with encryption, key management, anonymity, and continuous monitoring. Furthermore, users can locate their data and track its history using hash values, enhancing transparency and accountability. Overall, the system aims to provide a secure, transparent, and efficient platform for decentralized file sharing while ensuring user privacy and data integrity

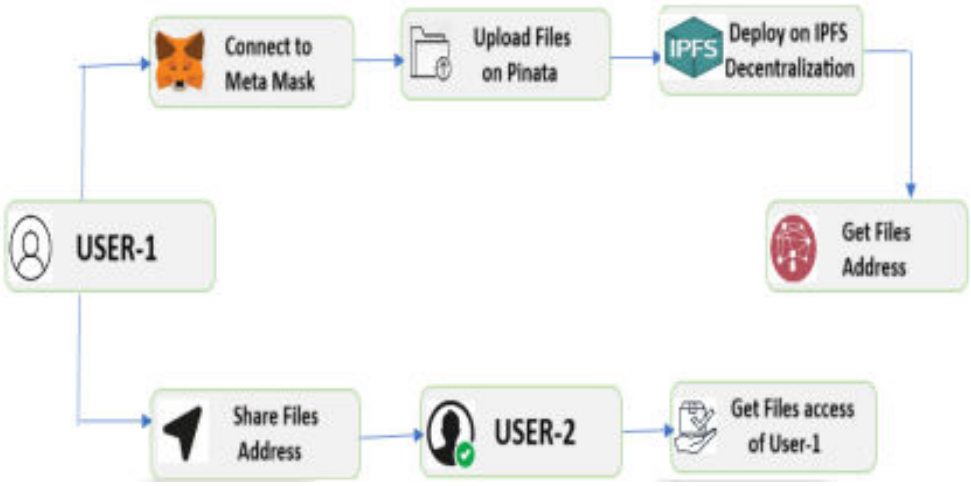
3.3 SYSTEM ARCHITECTURE

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 2, March-April 2026||

DOI:10.15662/IJRAI.2026.0902008



IV. SYSTEM IMPLEMETATION

4.1. MODULE:

1. User / Client Module
2. Encryption & Chunking Module (Client-Side)
3. Storage Node / Peer Module
4. Distributed Index & Metadata Module
5. Blockchain / Ledger Module
6. Incentive & Payment Module
7. Proof & Audit Module
8. Access Control / Key Management Module
9. Admin / Monitoring Module
10. Web / Mobile UI Module

4.2 MODULE DESCRIPTION:

1. User / Client Module

Handles user authentication, file upload/download requests, key management (generate/store private keys), UI interactions, and payment initiation. Performs client-side encryption and chunking before sending data to the network.

2. Encryption & Chunking Module (Client-Side)

Splits files into chunks, applies client-side symmetric encryption per chunk (e.g., AES-GCM), computes content hashes and Merkle roots, and prepares encrypted chunks for distribution. Generates metadata (chunk list, Merkle root, file size, content-type).

3. Storage Node / Peer Module

Runs on decentralized nodes that accept encrypted chunks, store and serve them, respond to retrieval requests, and participate in proof protocols. Nodes register availability, stake collateral (if applicable), and track storage contracts.

4. Distributed Index & Metadata Module

Maintains mappings from content hashes / Merkle root to storage node locations and metadata (replication factor, expiration). Can be implemented via a distributed hash table (DHT), IPFS-like index, or hybrid off-chain index with on-chain anchors.

5. Blockchain / Ledger Module

Stores immutable metadata anchors: file ownership, Merkle root, timestamp, storage contract references, payment receipts, and access-control policies. Facilitates dispute resolution and auditability. Smart contracts enforce staking, payments, and slashing rules.

6. Incentive & Payment Module

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 2, March-April 2026||

DOI:10.15662/IJRAI.2026.0902008

Handles payments between users and storage providers using on-chain tokens or off-chain micropayment channels. Manages escrow for storage duration, payouts upon successful proof, and penalties for proven downtime/data loss.

7. Proof & Audit Module
Implements Proof-of-Replication / Proof-of-Spacetime or challenge-response proofs. Periodic challenges verify nodes still store encrypted chunks; successful proofs trigger payouts; failures may trigger penalties recorded on-chain.

8. Access Control / Key Management Module
Manages encryption keys, key sharing, and revocation. Supports options like:

- Asymmetric envelope encryption (encrypt file key with recipient's public key)
- Proxy re-encryption for scalable sharing
- Attribute-based encryption for policy-based access

Key material is never stored on storage nodes.

9. Admin / Monitoring Module
Administration dashboard for monitoring node health, network capacity, payments, disputes, and logs. Provides analytics and alerts for anomalies.

10. Web / Mobile UI Module
User-friendly interfaces for uploading/downloading files, sharing links (with built-in decryption keys or keyless secure tokens), viewing storage contracts and balances, and managing account settings.

V. CONCLUSION

5.1 CONCLUSION

A Decentralized Secure File Storage Platform offers a privacy-first, resilient, and auditable alternative to centralized storage. By combining client-side encryption, distributed storage, on-chain metadata anchoring, incentive mechanisms and provable storage, the platform empowers users with ownership and control of their data while rewarding reliable storage providers. The hybrid off-chain/on-chain architecture balances performance with transparency, making this approach practical for real-world adoption in personal cloud storage, archival backup, enterprise compliance, and censorship-resistant content hosting.

REFERENCES

1. Howe, A. von Mayrhauser, and Mraz, R. T. Test case generation as an AI planning problem. Automated Software Engineering, 4:77-106, 1997.
2. Koehler, J., Nebel, B., Hoffman, J., and Dimopoulos, Y. Extending planning graphs to an ADL subset. Lecture Notes in Computer Science, 1348:273, 1997.
3. Treutner, M. F., and Ostermann, H. Evolution of Standard Web Shop Software Systems: A Review and Analysis of Literature and Market Surveys.
4. CS-Cart.com (Simbirsk Technologies Ltd), © 2004-2013.http://www.cs-cart.com/
5.Ofbiz, the Apache Open for Business Project. Retrieved on 2013."http://ofbiz.apache.org/index.html"
6.Comparison of shopping cart software. Retrieved on June 28, 2013.
http://en.wikipedia.org/wiki/Comparison_of_shopping_cart_software
7.Demonstrating how the web server Operates using PHP5/24/2018
8.All about frontend controls in php http://www.msdn.microsoft.com/
9.Wikipedia for various diagrams & testing methods http://www.wikipedia.org/
10.Cool text for Images and Buttons http://cooltext.com/
11.K-State Research Exchange for samples in report writing http://krex.k-state.edu/dspace/handle/2097/959
12. Smart Draw for drawing all the Diagrams used in this report. http://www.smartdraw.com/
13. Sample Ecommerce Application http://www.NewEgg.com
14. Ajax Toolkit controls http://asp.net/ajax