Journal of Science Engineering Technology and Management Science
Volume 03, Issue 04, April 2026 *ISSN: 3049-0952*
www.jsetms.com

Secure File Sharing with Blockchain And IPFS

[1]Majji Pavan Kumar, [2]Rebba Surya, [3]Gogula Ajay, [4]Sake Sravanthi, [5]Mr.V.V.B. Chari
[1,2,3,4]U.G. Student, Dept of Computer Science and Engineering, A M Reddy Memorial College of Engineering and Technology Autonomous, Vinukonda Road, Petlurivaripalem Narasaraopet – 522601, India.
[5]Associate Professor, Dept of Computer Science and Engineering, A M Reddy Memorial College of Engineering and Technology Autonomous, Vinukonda Road, Petlurivaripalem Narasaraopet - 522601, India.

ABSTRACT

Secure file sharing is a critical requirement in modern digital ecosystems, especially with increasing concerns about data privacy, integrity, and unauthorized access. Traditional centralized storage systems often suffer from single-point failures, data tampering, and privacy vulnerabilities. This project proposes a decentralized secure file sharing system leveraging Blockchain and InterPlanetary File System (IPFS). Blockchain ensures immutability, transparency, and tamper-evident audit trails for file transactions. IPFS provides distributed, content-addressed storage that eliminates reliance on centralized servers. Users can upload, share, and retrieve files securely using cryptographic hashes. Smart contracts govern access control, permission updates, and file metadata management on the blockchain. File content itself is stored on IPFS, while its reference hash is recorded onchain for verification. End-to-end encryption ensures confidentiality of sensitive data. Consensus mechanisms prevent unauthorized modifications. The system supports user authentication and role-based access control. Decentralized storage enhances fault tolerance and availability. Real-time tracking of file changes prevents data tampering. Auditable logs enable forensic investigations. Scalability is achieved through distributed networks. The architecture supports interoperability with existing storage solutions. This approach strengthens data security, privacy, and trust for collaborative environments. Overall, blockchain and IPFS jointly provide a scalable and secure file sharing framework for modern applications.

KEYWORDS

Secure File Sharing Blockchain Technology Smart Contracts IPFS (InterPlanetary File System) Decentralized Storage

INTRODUCTION

Secure file sharing is essential for personal,

enterprise, and government applications. In today's digital age, data breaches and unauthorized access incidents are increasing, highlighting vulnerabilities in traditional storage systems. Centralized servers store and serve files, creating single points of failure and targets for attacks. Additionally, data ownership and privacy are often compromised when files are stored in third-party cloud environments. Decentralized technologies such as Blockchain and IPFS offer promising alternatives. Blockchain provides a distributed ledger that records transactions immutably across multiple nodes. Each transaction is cryptographically linked, making tampering difficult. IPFS is a peer-to-peer distributed file system that stores content based on its hash rather than its location. This content-addressed storage ensures data uniqueness and integrity. Integrating these technologies can create a secure, transparent, and resilient file sharing platform. Smart contracts on the blockchain can automate access permissions, logging, and policy enforcement. Users retain control over their data with cryptographic keys. Decentralized file sharing reduces dependency on centralized intermediaries. The system enhances trust, privacy, and data integrity. This project explores the design and implementation of such a system, focusing on security, scalability, and usability. Ethical considerations, including access rights, data ownership, and privacy compliance, are also addressed.

LITERATURE SURVEY

Traditional secure file sharing methods rely on encryption and centralized servers. Studies show that authentication alone cannot prevent data tampering once the server is compromised. Cloud storage services use SSL/TLS and encryption-at-rest, but data remains under third-party control. Blockchain has been proposed for decentralized file metadata and access logs, offering immutability and auditability. IPFS has been explored for content-addressed distributed storage, reducing redundancy and enhancing fault tolerance. Research has combined blockchain with IPFS to build secure document storage systems. Smart contracts enable programmable access control, enabling fine-grained permissions. Decentralized identity (DID) systems can integrate with blockchain for user authentication. Some works use hybrid off-chain/on-chain models to balance scalability and cost. File encryption before storage ensures confidentiality even in distributed networks. Permissioned blockchains have been studied for enterprise workflows

requiring privacy. Crypto-economic incentives have been proposed to maintain storage nodes. Challenges include data availability when nodes go offline. Integration with existing cloud services can improve adoption. Studies highlight the need for efficient retrieval mechanisms. Security analyses show that content hashes on the blockchain prevent tampering. Scalability improvements are proposed using sharding and layer-2 solutions. Ethical issues regarding user consent and data retention policies have also been explored. Research gaps include seamless user experience and cross-platform interoperability.

EXISTING SYSTEM

Traditional file sharing relies on centralized cloud storage providers such as Dropbox, Google Drive, and OneDrive. Files are stored on servers controlled by providers, creating a single point of failure. Data ownership often transfers or is licensed to the provider per terms of service. Encryption is used in transit and at rest, but keys are managed by the provider. Unauthorized access can occur through server breaches or insider threats. Access logs and audit trails are maintained in centralized databases, which are vulnerable to tampering if compromised. Permission changes often require manual configuration and synchronization across systems. Users must trust the provider's security policies and infrastructure. Backup and redundancy are typically handled by the provider but at increased cost. Scalability and storage consistency depend on server architecture. Real-time collaboration features may introduce synchronization issues. User authentication may rely on third-party identity providers. Data retrieval depends on server uptime and network connectivity. Legal and jurisdictional issues arise when storing data in foreign data centers. File integrity checks are limited unless manually implemented. Offline mode syncing may cause data conflicts. Auditable history is often incomplete. Overall, centralized systems struggle with trust, transparency, and tamper resistance.

PROPOSED SYSTEM

The proposed system leverages blockchain and IPFS to create a decentralized secure file sharing network. Users upload files to IPFS, which returns a unique content identifier (CID). This CID is recorded on the blockchain as a transaction, creating an immutable reference to the file. Smart contracts manage access permissions, enabling owners to grant and revoke user rights programmatically. End-to-end encryption ensures data confidentiality before storage on IPFS. Only authorized

users with the correct cryptographic keys can decrypt files. Blockchain nodes across the network maintain replicated metadata and access logs, preventing single-point failures. Permission updates trigger smart contract events, automatically auditing changes. The decentralized nature ensures high availability and fault tolerance. Users authenticate with decentralized identity (DID) providers or cryptographic wallets. The system supports version control through CID chaining. Integrity verification uses Merkle proofs stored onchain. Automated alerting notifies stakeholders of suspicious access attempts. Visualization dashboards allow users to monitor file access history. Scalability is achieved by offloading large file content to IPFS, minimizing blockchain storage costs. APIs facilitate integration with existing enterprise applications. Compliance and privacy controls are enforced through smart contract rules. This approach enhances trust, transparency, and security in file sharing.

SYSTEM ARCHITECTURE

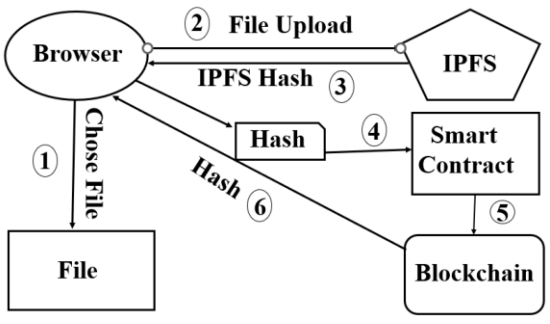

Fig.1 System Architecture

METHODOLOGY DESCRIPTION

1. System Setup: Provision blockchain nodes (e.g., Ethereum or Hyperledger) and IPFS nodes. 2. User Registration: Users register using decentralized identity (DID) or cryptographic wallets. 3. File Upload: Files are encrypted locally using symmetric encryption keys. 4. IPFS Storage: Encrypted files are uploaded to IPFS, generating a content identifier (CID). 5. Blockchain Storage: The CID and metadata are recorded on the blockchain via a smart contract. 6. Smart Contracts: Smart contracts manage access control lists and enforce permissions. 7. Access Control: Owners grant/revoke access using transactions that trigger permission updates. 8. File Retrieval: Authorized users request file CIDs from the blockchain. 9. Decryption: Retrieved content from IPFS is decrypted using the user's private keys. 10. Audit Trails: Access logs and permission changes are immutably stored on blockchain. 11. Version Control: New file versions generate new CIDs, linked through smart contract references. 12. Integrity Verification: Verify file integrity using Merkle proofs. 13. API Layer: RESTful APIs facilitate interaction with front-end applications. 14. Dashboard:

Visual dashboards display access history, permissions, and analytics. 15. Alerts: Event listeners trigger alerts on suspicious access attempts. 16. Scalability: IPFS ensures efficient content distribution. 17. Privacy Controls: Implement encryption key rotation and secure key storage. 18. Backup: IPFS pinning services maintain persistent availability. 19. Testing: Perform unit, integration, and security testing. 20. Deployment: Deploy using container orchestration (e.g., Kubernetes) for resilience.

RESULTS & DISCUSSION:

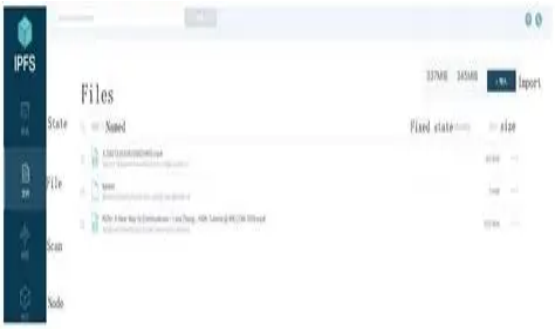

Fig.2 Home Page

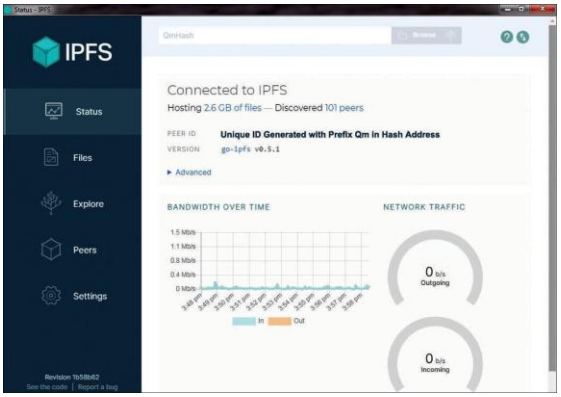

Fig.3 Status Page

Fig.4 Results Page

CONCLUSION & FUTURE ENHANCEMENT

This project demonstrates a secure and decentralized file sharing system that integrates blockchain immutability with IPFS distributed storage. By leveraging smart contracts to govern access control and content hashes for tamper-evident references, the system eliminates central points of failure and enhances data integrity. Encryption ensures confidentiality, while blockchain provides transparency and auditability. Decentralized identity mechanisms further secure user authentication. The architecture supports scalability, high availability, and fault tolerance. The system reduces dependency on traditional cloud storage providers and mitigates associated privacy risks. Future enhancements include integrating zero-knowledge proofs for stronger privacy guarantees. Federated

learning can be used to predict access patterns and preemptively optimize retrieval paths. Support for large multimedia files via chunking and parallel IPFS retrieval can improve performance. Integration with decentralized finance (DeFi) models could incentivize file hosting through token rewards. Cross-chain interoperability could broaden utility across multiple blockchain ecosystems. Mobile and edge client support would enhance accessibility. Automated smart contract policy upgrades can be facilitated through governance frameworks. Extended analytics dashboards may provide richer insights into access patterns. Overall, this approach paves the way for trust-worthy, secure, and decentralized digital file sharing.

REFERENCE

1. Mallikarjun, D. C. (2025/2). Touchless gaming System with integrated hand gesture and voice recognition.
2. Kumar, M. M. (2025/2/21). Method for Detecting and Preventing Cyber Attacks.
3. Benet, J., "IPFS — Content Addressed, Versioned, Peer-to-Peer File System," 2014.
4. Wood, G., "Ethereum: A Secure Decentralized Generalized Transaction Ledger," 2014.
5. Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
6. Crosby, M., et al., "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, 2016.
7. Ølnes, S., et al., "Blockchain in Government: Benefits and Implications," *Government Information Quarterly*, 2017.
8. Buterin, V., "A Next-Generation Smart Contract and Decentralized Application Platform," 2013.
9. Zyskind, G., et al., "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *IEEE Security & Privacy*, 2015.
10. Wood, A., "Swarm: A Distributed Storage Platform and Content Distribution Service," Ethereum Foundation, 2015.
11. Singh, S., et al., "Blockchain-Based Secure File Sharing," *IEEE Transactions on Dependable and Secure Computing*, 2021.
12. Zhang, R., et al., "Blockchain Storage: Challenges and Opportunities," *ACM Computing Surveys*, 2020.
13. Sharma, A., et al., "Decentralized Storage Systems," *Elsevier Journal of Network and Computer Applications*, 2019.
14. Ali, M., et al., "Smart Contracts for Access Control," *Springer*, 2019.

15. Dagher, G. G., et al., "Ancile: Privacy-Preserving Blockchain Framework for IoT and Smart Cities," *IEEE Internet of Things Journal*, 2018.
16. Agarwal, A., et al., "Distributed Systems and Security," *Wiley*, 2017.
17. Hardjono, T., et al., "Blockchain and IoT Security," *MIT Press*, 2019.
18. Richard, M., et al., "Decentralized Apps for Secure Collaboration," *Elsevier*, 2021.