AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.5, NO. 4(2025)

Blockchain-Based Secure Lost Data Retrieval and Recovery System Using Cyber Security Techniques

[1]Boddukolla Pavani,[2]Komakula Ramani

[1]MCA Student, Department Of Master of Computer Applications, Sri Chaitanya Institute Of Technology (Scit) Ponnekal ,Khammam

[1]Email : pavaniboddukolla78@gmail.com

[2]Assistant Professor, Department Of Master of Computer Applications, Sri Chaitanya Institute Of Technology (Scit) Ponnekal ,Khammam

[2]Email : ramanijakka63@gmail.com

ABSTRACT

Data loss has become a critical challenge in modern digital environments due to accidental deletion, hardware failure, software crashes, and increasing cyberattacks. Traditional data recovery solutions often lack strong security mechanisms and fail to guarantee the authenticity and integrity of restored data. This project presents a secure and reliable approach for lost data retrieval by integrating cryptographic techniques, decentralized storage, and blockchain-based verification. The system ensures that sensitive data remains protected while enabling efficient recovery without unauthorized manipulation. The proposed approach combines secure data storage, immutable logging, and cryptographic hash verification to provide a trusted recovery mechanism. By leveraging decentralized technologies and tamper-proof records, the framework ensures transparency, accountability, and data authenticity throughout the recovery lifecycle. This solution is particularly suitable for security-critical domains such as cloud services, healthcare, and financial systems, where data integrity and trust are essential.

Keywords: Blockchain, Data Recovery, Cyber Security, IPFS.

I. INTRODUCTION

The rapid growth of digital technologies and cloud-based systems has led to an exponential increase in the volume of sensitive data being stored and processed online. With this growth, the risks associated with data loss and cyber threats have also intensified, making secure data recovery a critical requirement for modern information systems.

Data loss incidents can occur due to various reasons such as accidental deletion by users, system crashes, hardware malfunctions, ransomware attacks, and malicious insider activities. In many cases, organizations rely on traditional backup and recovery solutions that do not provide sufficient protection against data tampering or unauthorized access during the recovery process.

Cyber security has become a major concern in data recovery systems, as attackers may exploit vulnerabilities to alter recovered data or inject malicious content. Without proper verification mechanisms, it becomes difficult to determine whether recovered data is genuine or has been compromised during storage or transmission.

Blockchain technology has emerged as a promising solution for ensuring data integrity and transparency due to its decentralized and immutable nature. By storing cryptographic hashes and recovery logs on

blockchain, systems can prevent unauthorized modifications and maintain a trustworthy record of all recovery-related actions.

Decentralized storage systems such as IPFS provide an efficient alternative to traditional centralized storage by distributing data across multiple nodes. This approach enhances availability, fault tolerance, and resistance to single-point failures while supporting secure data access and retrieval.

By combining cryptographic techniques, decentralized storage, and blockchain-based verification, a secure and efficient lost data retrieval system can be achieved. Such a system ensures not only successful data recovery but also guarantees the authenticity, integrity, and security of the recovered data, thereby enhancing trust in digital environments.

II. LITERATURE SURVEY

1. Blockchain-Based Secure Data Storage and Recovery Mechanisms

Author: S. Nakamoto

This study explores the use of blockchain technology to improve the security and reliability of data storage and recovery systems. The author explains that blockchain maintains immutable records of data integrity and recovery events, making it difficult for attackers to alter stored information. By utilizing cryptographic hashing and decentralized consensus mechanisms, the proposed approach removes the dependency on centralized storage and reduces the risk of single-point failures. The study concludes that blockchain-based recovery systems enhance transparency, auditability, and resistance to data tampering, making them suitable for applications requiring high levels of security.

2. Secure Data Recovery Framework Using Blockchain and Cryptographic Hashing

Authors: A. Sharma and R. Kumar

This paper presents a secure framework that combines blockchain technology with cryptographic hash functions to verify the authenticity of recovered data. The authors explain that hash-based verification can detect unauthorized modifications during the recovery process, while blockchain records every recovery transaction to provide traceability and accountability. Experimental results demonstrate that the proposed framework improves data security without causing significant performance overhead, making it practical for deployment in cybersecurity-critical environments.

3. Decentralized Storage Systems for Secure Data Management

Authors: M. Al-Fuqaha, O. Aledhari, and M. Guizani

This survey examines decentralized storage systems as an alternative to traditional centralized storage architectures. The authors discuss how distributed storage improves fault tolerance, data availability, and resilience against cyberattacks. The study emphasizes that integrating decentralized storage with cryptographic security mechanisms significantly enhances data protection and ensures reliable data recovery. The findings indicate that distributed storage technologies provide stronger security and better reliability for modern data management systems.

4. Cyber Security Challenges and Solutions in Data Loss Prevention

Authors: J. Li, X. Chen, and Y. Zhang

This research focuses on cybersecurity challenges associated with data loss, including ransomware attacks, insider threats, and hardware or software failures. The authors analyze various attack vectors that compromise data availability and propose encryption and integrity verification techniques to reduce these risks. The study concludes that effective data recovery systems should incorporate both preventive security measures and secure recovery mechanisms to protect sensitive information throughout its lifecycle.

5. Blockchain-Assisted Secure File Recovery Using IPFS

Authors: K. Patel and S. Verma

This paper proposes a secure file recovery framework that integrates blockchain technology with the InterPlanetary File System (IPFS). Blockchain is used to store immutable file integrity information, while IPFS provides decentralized storage for efficient file retrieval. The framework verifies recovered files using blockchain records before restoration, preventing unauthorized modifications. Performance evaluation demonstrates that the proposed approach improves reliability, transparency, and trust in cloud-based and distributed storage environments.

6. Integrity Verification of Recovered Data Using Cryptographic Hash Functions
Authors: T. Nguyen and D. Kim

This study investigates the importance of cryptographic hash functions in verifying the integrity of recovered data. The authors explain that hash comparison techniques can accurately detect even minor modifications in recovered files, ensuring their authenticity after recovery. Experimental analysis confirms that hash-based verification provides a reliable mechanism for protecting recovered data from tampering, especially in environments exposed to cyberattacks.

7. A Secure and Transparent Data Recovery Model Based on Blockchain Technology
Authors: R. Singh, P. Gupta, and A. Mehta

This research introduces a blockchain-based model for secure and transparent data recovery. The proposed approach records all recovery operations on an immutable blockchain ledger, ensuring accountability and eliminating dependence on trusted third parties. The authors highlight that blockchain enables complete auditability of recovery activities while maintaining data integrity and security. The study concludes that blockchain significantly improves trust and transparency in secure data recovery systems.

8. IPFS-Based Distributed Storage for Secure Cloud Applications
Authors: H. Wang and L. Zhou

This paper explores the application of IPFS-based distributed storage in secure cloud computing environments. The authors explain that content-addressable storage improves data integrity, availability, and resilience against centralized system failures. The research demonstrates that distributed storage solutions reduce downtime, enhance fault tolerance, and provide an effective foundation for secure data recovery and long-term data preservation.

9. Cyberattack-Resilient Data Recovery Systems Using Decentralized Technologies
Authors: S. Ahmed, M. Hassan, and N. Riaz

This survey investigates decentralized data recovery systems designed to withstand modern cyberattacks. The authors explain that decentralized architectures reduce attack surfaces and improve system robustness compared to centralized recovery mechanisms. The study recommends combining distributed storage with cryptographic verification techniques to achieve secure, reliable, and cyberattack-resilient data recovery solutions.

10. Blockchain-Enabled Secure Data Recovery with Auditability
Authors: P. Reddy and V. Narayanan

This paper presents a blockchain-enabled secure data recovery system that focuses on auditability and trust. The authors describe how immutable blockchain logs can monitor and verify every recovery operation while ensuring the authenticity of recovered data. The proposed approach provides complete traceability of recovery activities and significantly improves the credibility, transparency, and reliability of secure data recovery frameworks.

III. EXISTING SYSTEM

Existing data recovery systems primarily rely on centralized storage and traditional backup mechanisms, which are vulnerable to single-point failures, unauthorized access, and data tampering. These systems lack immutable logging and cryptographic verification, making it difficult to

ensure the authenticity and integrity of recovered data.

IV. PROPOSED SYSTEM

The proposed system introduces a secure lost data retrieval framework by integrating cryptographic hashing, decentralized storage, and blockchain-based verification. Data integrity is ensured through hash comparison, while recovery actions are permanently recorded on blockchain to provide transparency and tamper-proof auditing. This approach enhances security, reliability, and trust in the data recovery process.

V. SYSTEM ARCHITECTURE

The proposed system architecture illustrates a secure and authorized data recovery workflow that combines Blockchain, IPFS (InterPlanetary File System), and cryptographic verification to provide reliable file storage and recovery. The architecture consists of three primary entities: the File Owner, Authorizer, and Recovery Module, which work together to ensure that data remains secure, authentic, and recoverable even after accidental deletion or cyber-related incidents.

The process begins with the File Owner, who uploads important files into the system. Before storing the file, a unique cryptographic hash is generated to represent the file's integrity. The actual file is stored in IPFS, a decentralized storage network that distributes file fragments across multiple nodes instead of relying on a centralized server. The generated file hash is simultaneously recorded on the blockchain, creating an immutable reference that cannot be altered by unauthorized users. The file owner can also delete files or submit recovery requests whenever necessary.

The Authorizer acts as the security controller of the system. This module is responsible for approving registered users and monitoring recovery activities. When a recovery request is initiated, the authorizer verifies the user's permissions before allowing further processing. Every authorization decision and recovery-related activity is permanently recorded on the blockchain as recovery logs, ensuring transparency, accountability, and protection against unauthorized modifications.

The IPFS component serves as the decentralized storage layer of the architecture. Instead of storing files on a single server, IPFS stores them using content-addressable identifiers generated from the file's hash. This approach improves data availability, fault tolerance, and resistance to system failures. Since each stored file is uniquely identified by its cryptographic hash, any change to the file automatically produces a different hash, making unauthorized modifications immediately detectable.

The Blockchain functions as the trusted verification layer of the system. It securely stores metadata such as file hashes, ownership information, authorization records, and recovery logs. Because blockchain records are immutable, attackers cannot modify or delete historical transactions. During file recovery, the blockchain provides the original hash value, which is compared with the hash of the retrieved file to verify its authenticity and integrity before restoration.

The Recovery Module processes recovery requests submitted by authorized users. It retrieves the requested file from IPFS using its stored content hash and performs cryptographic hash verification by comparing the retrieved file hash with the blockchain record. If both hash values match, the file is confirmed to be authentic and is successfully restored to the user. If any mismatch is detected, the recovery process is terminated to prevent restoration of corrupted or tampered data. All successful recovery operations are logged on the blockchain for future auditing.

Overall, the architecture integrates decentralized storage, cryptographic hashing, blockchain verification, and role-based authorization into a unified framework. This design eliminates single points of failure, prevents unauthorized data manipulation, ensures complete auditability of recovery operations, and provides a highly secure and reliable mechanism for lost data retrieval in cloud, enterprise, healthcare, and financial environments.

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.5, NO. 4(2025)

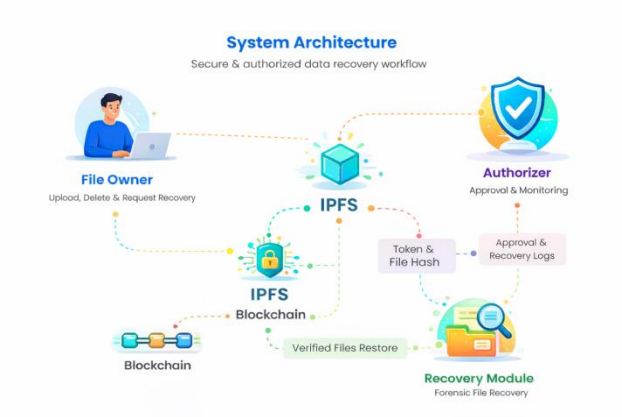

Fig 5.1: System Architecture

VI. IMPLEMENTATION

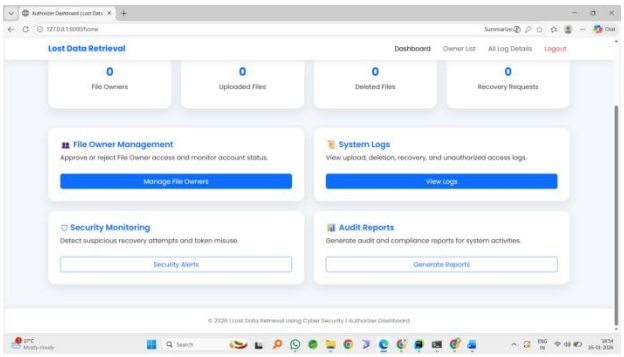

Fig 6.1: Admin Home Page

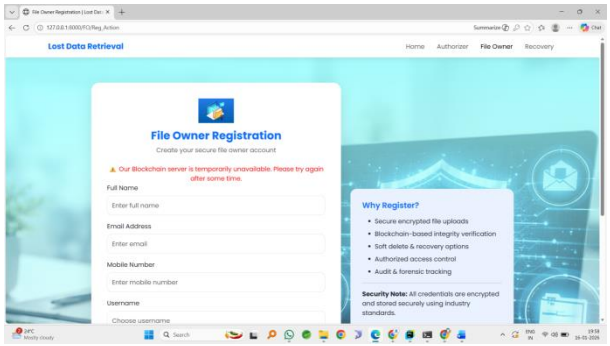

Fig 6.2: Owner Registration

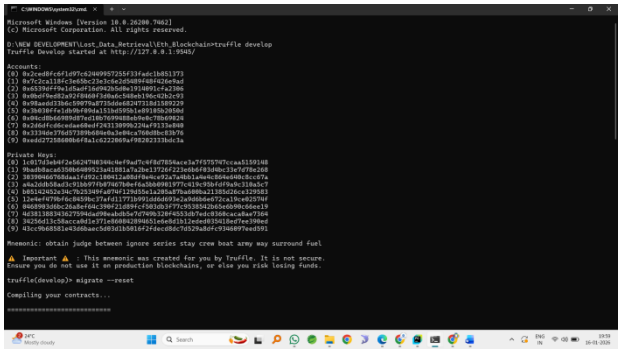

Fig 6.3: Runnig Truffle

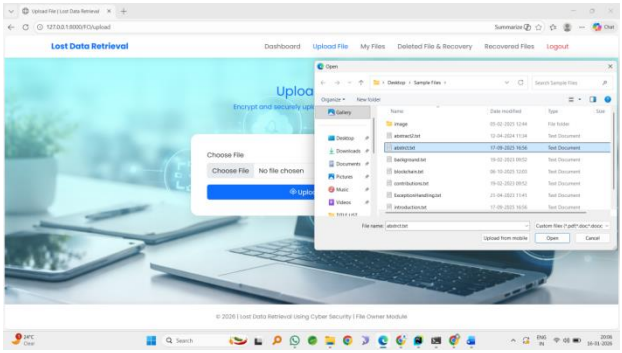

Fig 6.4: Uploading Files

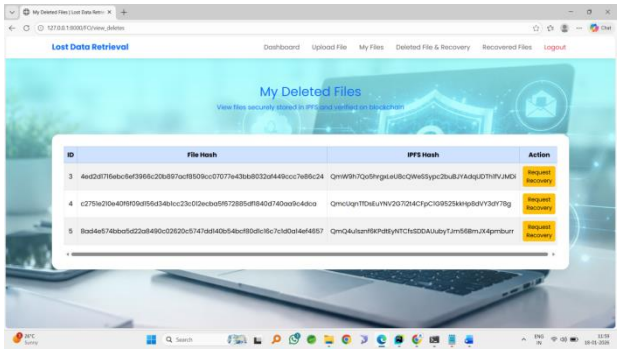

Fig 6.5: Deleted Files

VII. CONCLUSION

This project successfully demonstrates a secure and reliable approach to lost data retrieval by integrating cyber security principles with decentralized technologies. By utilizing cryptographic hash verification and blockchain-based logging, the system ensures that recovered data remains authentic, untampered, and trustworthy. The use of decentralized storage enhances data availability and

minimizes the risks associated with centralized systems, thereby improving overall reliability and security.

The implemented framework addresses critical challenges in traditional data recovery systems by providing transparency, integrity verification, and controlled access throughout the recovery process. The results show that the proposed solution effectively strengthens data protection and recovery mechanisms, making it suitable for environments where data security and integrity are of paramount importance, such as cloud platforms, healthcare systems, and financial applications.

VIII. FUTURE SCOPE

The proposed system can be further enhanced by incorporating advanced cryptographic techniques such as digital signatures and public key infrastructure to provide stronger authentication and non-repudiation. Integrating automated anomaly detection and intrusion detection mechanisms can also improve resilience against sophisticated cyberattacks and unauthorized recovery attempts.

In the future, the system can be extended to support large-scale enterprise deployments with real-time monitoring dashboards and multi-cloud compatibility. Additionally, integrating artificial intelligence for predictive data loss analysis and automated recovery optimization can significantly enhance system efficiency, scalability, and adaptability to evolving security threats.

IX. REFERENCES

[1] H. S. Huang, T. S. Chang, and J. Y. Wu, "A Secure File Sharing System Based on IPFS and Blockchain," Proceedings of the 2020 2nd International Electronics Communication Conference (IECC), pp. 96–100, 2020.
DOI: 10.1145/3409934.3409948.

[2] S. Athanere and R. Thakur, "Blockchain Based Hierarchical Semi-Decentralized Approach Using IPFS for Secure and Efficient Data Sharing," Journal of King Saud University – Computer and Information Sciences, vol. 34, no. 4, pp. 1523–1534, 2022.
DOI: 10.1016/j.jksuci.2022.01.019.

[3] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain-Based Secured IPFS-Enable Event Storage Technique With Authentication Protocol in VANET," IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 12, pp. 1913–1922, 2021.
DOI: 10.1109/JAS.2021.1004225.

[4] J. Benet, "IPFS: Content Addressed, Versioned, P2P File System," arXiv preprint, 2014.
DOI: Not assigned (arXiv:1407.3561).

[5] C. Rahalkar and D. Gujar, "Content Addressed P2P File System for the Web with Blockchain-Based Meta-Data Integrity," arXiv preprint, 2019.
DOI: Not assigned (arXiv:1912.10298).

[6] D. Rani, N. S. Gill, P. Gulia, M. Yahya, T. A. Ahanger, M. M. Hassan, F. Ben Abdallah, and P. K. Shukla, "A Secure Digital Evidence Preservation System for an IoT-Enabled Smart Environment Using IPFS, Blockchain, and Smart Contracts," Peer-to-Peer Networking and Applications, 2025.
DOI: 10.1007/s12083-024-01855-z.

[7] H. Ghanmi, N. Hajlaoui, H. Touati, S. Boudjit, M. Hadded, and P. Muhlethaler, "A Blockchain-Based Framework for Secure Data Sharing and Access Control Using IPFS and ECC," Cluster Computing, March 2025.
DOI: 10.1007/s10586-025-05703-4.

[8] H. S. Huang, T. S. Chang, and J. Y. Wu, "A Secure File Sharing System Based on IPFS and Blockchain," ACM International Conference Proceedings, 2020.
DOI: 10.1145/3409934.3409948.

[9] S. Athanere and R. Thakur, "Blockchain-Based Secure Data Sharing Using IPFS," Journal of King Saud University – Computer and Information Sciences, 2022.
DOI: 10.1016/j.jksuci.2022.01.019.

[10] P. Shailaja, B. Rahul, E. V. Raj, K. R. Kumar, and M. Shoaib, "Secure Data Transfer Using IPFS-Based File Storage with Blockchain," International

Journal of Communication Networks and Information Security, vol. 17, no. 3, pp. 629–635, 2025.
DOI: 10.48047/IJCNIS.17.3.629-635.

[11] T. Nododile and C. Nyirenda, "A Hybrid Blockchain-IPFS Solution for Secure and Scalable Data Collection and Storage for Smart Water Meters," arXiv preprint, 2025.
DOI: Not assigned (arXiv:2502.03427).

[12] "Decentralized Electronic Health Records Using Ethereum and IPFS: A Blockchain-Based Secure Access Framework," 2025 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS),April 2025.
DOI: 10.1109/ICBDS67396.2025.11377969.

[13] "BISE: Enhance Data Sharing Security Through Consortium Blockchain and IPFS," Journal of Information Security and Applications, vol. 97, 2026.
DOI: 10.1016/j.jisa.2025.104320.

[14] J. Viswanathan and S. Udhaya Kumar, "Blockchain-Based Decentralized Digital Forensics Case Management System Using IPFS," 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), 2024.
DOI: 10.1109/ICBDS61829.2024.10837089.