International Journal of Computer Science Engineering Techniques (IJCSE) Volume 10 Issue 2 ,Mar-Apr 2026

ISSN : 2455-135X

AI-Driven Secure File Storage System Using Blockchain with Real-Time Anomaly Detection

Muthupandi M[1], Kamalesh S[2], Santhoshkumar R[3] , Saminathan S [4]

[1,2,3,4]*Department of Computer Science and Engineering, N.S.N. College of Engineering and Technology, Karur, Tamil Nadu, India.*

muthupandi.m1545@gmail.com

Received: 17 April 2026 Revised: Accepted: Published:

Abstract - *In the era of digital transformation, ensuring the security of stored data has become increasingly challenging due to the rise in sophisticated cyber threats. This paper introduces an intelligent file storage framework that combines encryption techniques, blockchain-based access control, and artificial intelligence-driven anomaly detection to enhance data security. The proposed system encrypts files before storage, ensuring confidentiality, while blockchain mechanisms are used to validate ownership and control access in a decentralized manner. Additionally, a real-time risk assessment engine continuously monitors user behavior to identify suspicious activities. Upon detecting anomalies, the system initiates automated defensive actions such as access denial, IP blocking, file quarantine, and alert notifications. A centralized dashboard is also provided to visualize system activity and threat levels. The experimental outcomes indicate that the proposed framework significantly improves protection against unauthorized access and cyber attacks, making it suitable for modern secure storage environments.*

Keywords - *anomaly detection, artificial intelligence, blockchain, cybersecurity, secure file storage, zero trust architecture*

1. Introduction

The rapid adoption of cloud-based storage systems has increased the need for robust data security mechanisms. Traditional storage solutions primarily rely on static authentication methods, which are insufficient against modern cyber threats such as unauthorized access, brute force attacks, and data tampering.

To address these limitations, there is a growing interest in integrating advanced technologies such as blockchain and artificial intelligence into security frameworks. Blockchain enables decentralized and tamper-resistant access control, while AI techniques can analyse user behaviour patterns and detect anomalies in real time.

This paper presents a secure file storage framework that integrates encryption, blockchain-based verification, and AI-driven intrusion detection. The system follows a Zero Trust approach, where every access request is validated regardless of its origin. By combining multiple layers of security, the proposed solution aims to provide a resilient and adaptive defense mechanism for protecting sensitive data**.**

2. Proposed System

2.1. File Encryption Module

All uploaded files are encrypted before being stored in the system. This ensures that even if unauthorized access occurs, the data remains protected and unreadable

2.2. Blockchain – Based Access Control

Each file is associated with a unique owner identity, verified through a blockchain mechanism. Access requests are validated against stored ownership data, preventing unauthorized users from retrieving files.

2.3. Anomaly Detection Engine

An AI-based module continuously monitors user behaviour, including access frequency and failed attempts. If abnormal patterns are detected, the system flags the activity as suspicious.

2.4. Risk Assessment Mechanism

A dynamic risk score is calculated for each user based on behavioural factors. This score determines the level of threat and triggers appropriate security actions.

2.5. Automated Response System

Depending on the severity of the detected threat, the system performs actions such as:

- *Blocking suspicious IP addresses*
- *Moving compromised files to quarantine*

ISSN : 2455-135X

- *Deleting files under extreme risk conditions*

3. System Architecture

The system follows a structured workflow where users first authenticate using a secure login mechanism. Uploaded files are encrypted and stored securely. During download requests, blockchain verification and anomaly detection are performed before granting access. The risk engine evaluates each request and determines whether to allow, block, or escalate the action.

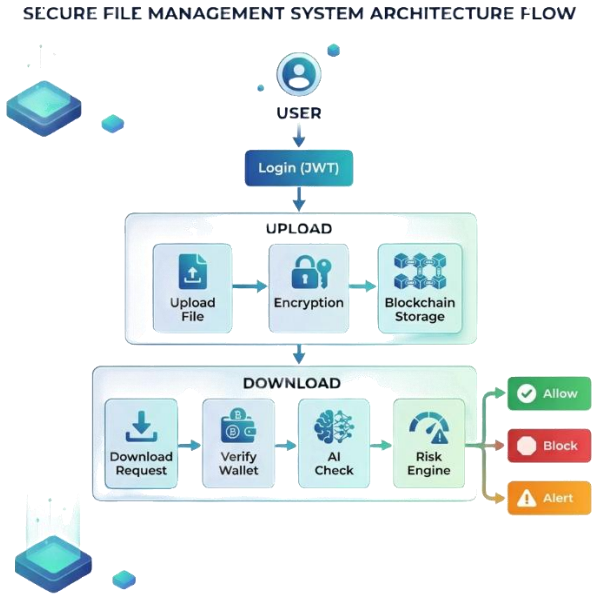

Fig. 1. Secure File Management System Architecture Flow

4. Implementation

The system is implemented using Python with the Flask framework for backend development. JWT-based authentication is used to manage secure user sessions. The blockchain component is implemented through a custom verification module that validates file ownership. The user interface is developed using HTML and CSS.

5. Results and Analysis

The proposed system was tested under various scenarios, including normal usage and simulated attack conditions. The results demonstrate that:

- Unauthorized access attempts were successfully detected and blocked
- Suspicious activities were identified within a short time frame
- Risk-based actions effectively prevented potential data breaches
- Real-time alerts enabled quick response to security threats

Overall, the system showed improved resilience compared to traditional storage methods, particularly in detecting and mitigating cyber attacks.

6. Conclusion

This paper presents a secure and intelligent file storage framework that integrates encryption, blockchain, and AI-based anomaly detection. The system provides multiple layers of security, ensuring data protection against unauthorized access and malicious activities. By incorporating real-time monitoring and automated response mechanisms, the proposed solution enhances both security and system reliability. The approach demonstrates strong potential for application in modern cloud storage and enterprise security systems.

7. Future Work

Future improvements may include:

- Integration of advanced machine learning models for better prediction accuracy
- Implementation of multi-factor authentication mechanisms
- Deployment on cloud platforms for scalability
- Real-time geolocation-based attack visualization
- Expansion to enterprise-level multi-user environments

Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

Funding Statement

This research received no external funding.

Acknowledgments

The authors would like to express their sincere gratitude to all individuals and resources that contributed to the successful completion of this work. We extend our appreciation to the faculty members and mentors who provided valuable guidance and technical insights throughout the development of this project. We also acknowledge the support of open-source communities and publicly available research materials that helped in understanding advanced concepts related to cybersecurity, blockchain technology, and machine learning. Finally, we thank our peers and well-wishers for their continuous encouragement and constructive feedback, which significantly improved the quality of this work.

ISSN : 2455-135X

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[2] D. Boneh and V. Shoup, "A Graduate Course in Applied Cryptography," 2020.
[3] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
[4] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," IEEE Symposium on Security and Privacy, 2010.
[5] National Institute of Standards and Technology (NIST), "Guide to Intrusion Detection and Prevention Systems (IDPS)," 2012.
[6] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," IEEE Communications Surveys & Tutorials, 2018.
[7] Scikit-learn Developers, "Anomaly Detection Techniques," [Online]. Available: https://scikit-learn.org
[8] OWASP Foundation, "OWASP Top 10 Web Application Security Risks," 2021.
[9] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Advances in Cryptology, 1984.
[10] J. Andress, "The Basics of Information Security," Elsevier, 2014.