International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 02 | Feb 2026 www.irjet.net p-ISSN: 2395-0072

BLOCKCHAIN ENABLED SECURE CLOUD STORAGE FOR CRIMINAL EVIDENCE

Mr. J. Ramesh[1], M.Gayathri[2], Sravani Sajjan[3], M. Shivani[4], Md Fareed Baba[5]

[1]*Asst.Professor in Department of IT, TKR College of Engineering and Technology, Telangana, India*
[2345] *BTECH Students in Department of IT, TKR College of Engineering and Technology, Telangana, India*

Abstract – *The increasing reliance on digital evidence in legal investigations demands secure and tamper-proof storage solutions. This project presents a Digital Evidence Management System (DEMS) that ensures the integrity, authenticity, and traceability of digital files using SHA-256 hashing. The system allows users to register, upload files, and generate unique hash keys for each uploaded evidence. Admins have control over user management, including account activation, deactivation, and monitoring of all uploaded files. When a user uploads a file for verification, the system computes its SHA-256 hash and compares it with existing entries in the database, thereby detecting any tampering or alteration. The uploaded files, along with associated metadata such as file name, uploader, timestamp, and hash key, are stored securely in a local media folder, ensuring organized evidence management. The platform also incorporates a secure password recovery mechanism using email-based OTP verification. By integrating file hashing with a robust user management framework, the system offers a reliable and efficient solution for managing digital evidence in investigations and legal proceedings. This approach provides a lightweight, blockchain-inspired model for evidence integrity without requiring a full blockchain implementation, making it practical for small- to medium-scale investigative workflows.*

Key Words: Digital Evidence, SHA-256, File Verification, Tamper Detection, Evidence Management System, Django.

1. INTRODUCTION

In modern legal and investigative processes, digital evidence has become a crucial component in establishing facts and proving cases. With the proliferation of digital data, the integrity, authenticity, and traceability of such evidence are paramount. Traditional methods of evidence storage often involve manual handling, centralized databases, or unprotected file systems, which are vulnerable to tampering, accidental loss, or unauthorized access. Any alteration in the digital evidence can compromise investigations and lead to legal challenges. To address these challenges, the Digital Evidence Management System (DEMS) integrates SHA-256 hashing to secure files uploaded by authorized users. Each file is processed to generate a unique hash key that acts as a digital fingerprint, ensuring that even minor modifications are detectable. The system incorporates robust user management, where admin approval is required for new users, and allows admins to monitor and manage all uploaded evidence. Users can verify the authenticity of a file at any time by re-uploading it for hash comparison, ensuring the evidence has not been altered. This approach provides a lightweight, blockchain-inspired solution for evidence security, offering high reliability without the complexity of full-scale blockchain implementation. By combining file integrity verification, controlled access, and centralized metadata storage, the system provides an efficient and trustworthy platform for managing digital evidence in investigations and legal proceedings.

1.1 Need for Secure and Tamper-Proof Criminal Evidence Management

In modern criminal investigations, digital evidence such as CCTV footage, forensic reports, call records, and cyber logs plays a crucial role in solving cases and ensuring justice. However, traditional evidence storage systems—often centralized or manually managed—are vulnerable to data breaches, unauthorized access, manipulation, and accidental loss. Even a minor alteration in evidence can compromise its integrity, leading to legal disputes and weakening its admissibility in court. To maintain the chain of custody, criminal evidence must remain confidential, immutable, and verifiable from the moment of collection to its presentation in court. As the volume of digital evidence grows rapidly, law enforcement agencies require a robust system that ensures long-term preservation, traceability, and accountability while preventing tampering and insider threats. This challenge has highlighted the need for advanced security mechanisms beyond conventional databases.

1.2 Role of Blockchain and Cloud in Enhancing Evidence Security

Blockchain technology offers a decentralized and immutable ledger that can significantly enhance the security of criminal evidence storage. By recording cryptographic hashes of evidence files on the blockchain, any unauthorized modification can be instantly detected, ensuring authenticity and non-repudiation. Each transaction related to evidence access, transfer, or modification is time-stamped and transparently logged, strengthening trust among law enforcement agencies, forensic departments, and judicial authorities.

Cloud computing complements blockchain by providing scalable, cost-effective, and highly available storage infrastructure for large volumes of evidence data. When integrated with blockchain, secure cloud storage enables encrypted evidence files to be stored efficiently while blockchain maintains proof of integrity and access control. This hybrid approach ensures confidentiality, integrity, availability, and auditability, making it an ideal solution for managing sensitive criminal evidence in a legally compliant and technologically advanced manner.

2. PROPOSED SYSTEM

The proposed system, Digital Evidence Management System (DEMS), is designed to securely store, manage, and verify digital evidence in investigative and legal environments. The system addresses the limitations of traditional centralized storage, including vulnerability to tampering, accidental loss, and unauthorized access. Each evidence file uploaded by a user is processed using SHA-256 hashing to generate a unique digital fingerprint, ensuring its integrity and authenticity. Metadata such as the uploader's details, file name, timestamp, and hash key is stored in the database for audit and verification purposes. The system incorporates role-based access control, where administrators approve new users, manage accounts, and monitor all uploaded evidence. Users can upload new files, verify existing evidence by uploading it for hash comparison, and receive immediate feedback on whether the file matches stored records. Password recovery is implemented via secure email based OTP verification to enhance usability. By combining hash-based verification with controlled access and centralized metadata management, the proposed system provides a lightweight, blockchain-inspired approach to tamper-proof digital evidence handling. It ensures reliability, traceability, and accountability, making it suitable for law enforcement agencies, forensic investigations, and other scenarios where the authenticity of digital evidence is critical. The system is scalable, efficient, and practical for both small- and medium-scale deployments.

2.1 System Architecture

The system architecture of the Blockchain Enabled Secure Cloud Storage for Criminal Evidence is designed as a layered and modular framework to ensure confidentiality, integrity, and traceability of digital evidence. At the front end, authorized users such as law enforcement officers, forensic experts, and judicial authorities interact with the system through a secure web interface with multi-factor authentication. Once evidence is uploaded, it is encrypted using strong cryptographic algorithms and stored in a secure cloud and case ID is generated and recorded on the blockchain network. Smart contracts manage access control, evidence lifecycle, and logging of all transactions, ensuring an immutable audit trail. Any request to access or modify evidence is verified against blockchain records, and integrity checks are performed by comparing stored hashes. This integrated architecture combines cloud storage efficiency with blockchain immutability, thereby maintaining an unbroken chain of custody and preventing unauthorized tampering of criminal evidence.

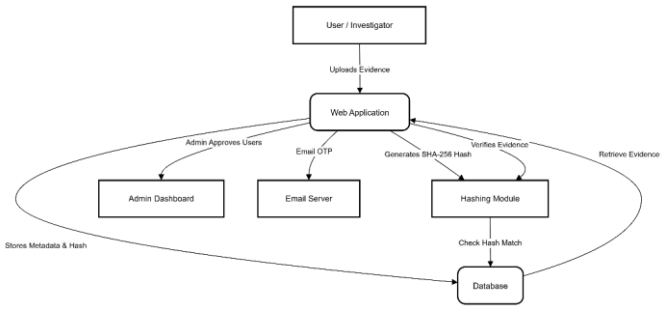

Fig -1 : System Architecture

2.2 Evidence Encryption and Secure Cloud Storage Layer

In the proposed system, all criminal evidence is secured before storage through strong encryption mechanisms to ensure confidentiality and prevent unauthorized access. When evidence such as images, videos, or documents is uploaded, it is encrypted at the client or application layer using cryptographic algorithms. The encrypted data is then stored in a secure cloud storage environment, which provides scalability, high availability, and reliable backup. This layer ensures that even if cloud infrastructure is compromised, the actual evidence remains unreadable without proper decryption keys. Secure cloud storage also enables efficient handling of large volumes of digital evidence while supporting controlled access based on user roles defined in the system.

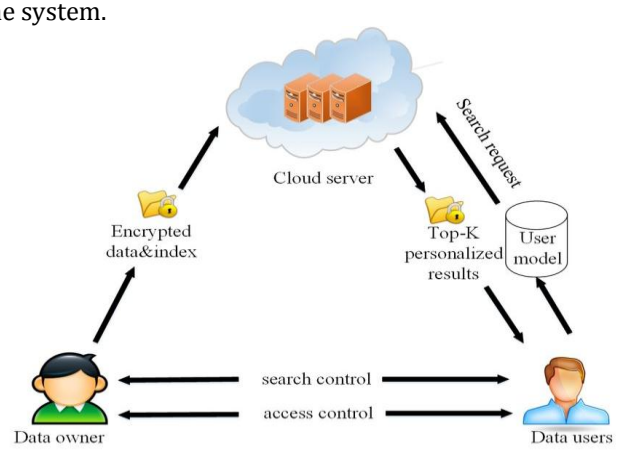

Fig-2 : Privacy-Preserving Search over Encrypted Cloud Data Architecture

2.3 Blockchain Layer for Integrity Verification and Audit Trail

The blockchain layer acts as the core trust mechanism of the proposed architecture by maintaining the integrity and traceability of criminal evidence. Instead of storing the actual evidence data on the blockchain, cryptographic hash values of the encrypted files along with metadata such as case ID, uploader identity, and timestamps are recorded. Each block is linked to the previous one, making the stored records immutable and tamper-proof. Smart contracts regulate access permissions and automatically log every evidence-related transaction, including uploads, access requests, and verification events. This creates a transparent and verifiable audit trail, ensuring an unbroken chain of custody and enhancing the legal admissibility of digital evidence.

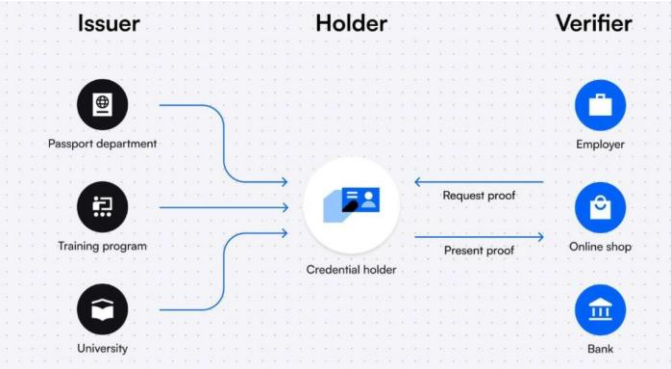

Fig-3: Self-Sovereign Identity (SSI) Credential Verification Model

3. IMPLEMENTATION DETAILS

It describes the practical steps to build a secure, auditable, tamper-evident evidence management system that combines cloud storage, cryptographic hashing, and blockchain notarization. The implementation plan follows a modular, testable approach so each component (ingestion, storage, verification, access control, blockchain anchoring, and audit) can be developed, validated, and integrated. The system's goal is to guarantee integrity, chain-of-custody, confidentiality, and controlled access for digital evidence used in legal proceedings. The implementation converts the architecture and designs into working modules: Evidence Ingestion, Hashing & Notarization, Off-chain Storage (cloud/IPFS), Permissioned Blockchain Layer, Access & Forensics Services, and Audit & Monitoring.

3.1 System Architecture Implementation

Implement using a layered architecture: Presentation (Frontend), Application (APIs & microservices), Data (cloud storage + metadata DB), Block chain (permissioned ledger), Security (authentication, encryption, login).

3.2 Frontend Layer

Build a responsive web UI (and optional mobile client) for: Evidence upload forms with metadata capture (case id, uploader, timestamp, device info, chain-of-custody notes). Evidence browsing, search, and filtered views for authorized roles. Forensic tools UI: file preview, hash verification, timeline view of custody events. Implement client-side hashing (optional) to show user-generated hash before upload. Communicate with backend via secure REST/GraphQL and WebSocket for live updates.

4. RESULTS AND PERFORMANCE ANALYSIS

The experimental results demonstrate that the proposed Blockchain Enabled Secure Cloud Storage for Criminal Evidence system effectively ensures data integrity, security, and reliable evidence management with acceptable performance overhead. During evaluation, evidence upload and retrieval operations showed minimal latency increase due to encryption and blockchain hash generation, while remaining within practical limits for real-world law enforcement use. Integrity verification tests confirmed that any unauthorized modification of stored evidence was immediately detected through hash mismatch, validating the immutability provided by the blockchain layer. The system also exhibited high reliability and availability due to cloud-based storage, even under increasing data volumes. Performance analysis indicates that while blockchain transaction processing introduces slight computational overhead, the benefits of tamper-proof audit trails, secure access control, and maintained chain of custody significantly outweigh the costs. Overall, the results confirm that the proposed architecture achieves a balanced trade-off between strong security guarantees and efficient system performance, making it suitable for secure criminal evidence management.

5. CONCLUSIONS

This project successfully presents a Blockchain Enabled Secure Cloud Storage for Criminal Evidence system that addresses critical challenges related to evidence security, integrity, and chain of custody in modern criminal investigations. By integrating strong encryption, cloud-based storage, and blockchain technology, the proposed system ensures that digital evidence remains confidential, tamper-proof, and verifiable throughout its lifecycle. The use of blockchain to store cryptographic hashes and access logs provides transparency, immutability, and trust among law enforcement and judicial authorities, while cloud infrastructure offers scalability and high availability. Overall, the proposed solution enhances the reliability and legal admissibility of criminal evidence and demonstrates the effectiveness of blockchain–cloud integration as a robust approach for secure evidence management in real-world scenarios.

6. FUTURE WORK

The proposed Blockchain Enabled Secure Cloud Storage for Criminal Evidence system can be further enhanced and expanded to address evolving technological and legal requirements. Future work may include the integration of advanced cryptographic techniques such as post-quantum encryption to strengthen long-term security. Incorporating artificial intelligence and machine learning models for automated evidence classification, anomaly detection, and tamper prediction can improve investigation efficiency. The system can also be extended to support multimedia forensic data such as real-time CCTV feeds, body-worn camera recordings, and IoT-based evidence. Additionally, deploying the solution on a consortium or permissioned blockchain across multiple law enforcement agencies can improve interoperability and trust while ensuring regulatory compliance. These enhancements would make the system more intelligent, scalable, and adaptable for next-generation digital forensic applications.

ACKNOWLEDGEMENT

There are many individuals who have contributed directly and indirectly to the successful completion of this project, and we take this opportunity to express our sincere gratitude to all of them. We are extremely thankful and indebted to our project supervisor, Mr. J. Ramesh, Assistant Professor, Department of Information Technology, TKR College of Engineering and Technology, for his constant guidance, encouragement, and moral support throughout the project. We also express our heartfelt thanks to Dr. R. Muruganantham, Head of the Department, Department of Information Technology, for his continuous encouragement and support. We are sincerely grateful to Dr. D. V. Ravi Shankar, Principal, TKR College of Engineering and Technology, for his timely support and valuable suggestions during the course of the project. Finally, we extend our thanks to all the faculty and staff of the Department of Information Technology, as well as our parents and friends, whose cooperation and support played a vital role in the successful completion of this project.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Cryptography Mailing List, 2008. DOI: 10.1007/978-3-662-53357-4_8

[2] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review, vol. 2, pp. 6–19, 2016.
DOI: 10.48550/arXiv.1510.03520

[3] A. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," IEEE Security and Privacy Workshops, 2015. DOI: 10.1109/SPW.2015.27

[4] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," IEEE Conference onSmartCities,2016.
DOI: 10.1109/ICSCC.2016.7919677

[5] S. Wang, Y. Zhang, and Y. Zhang, "A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems," IEEE Access, vol. 6, pp. 38437–38450, 2018. DOI: 10.1109/ACCESS.2018.2851611

[6] H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering Blockchain-Based Cloud Data Provenance," IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3183–3195,2019.
DOI: 10.1109/TII.2018.2878840

[7] Y. Zhang, J. Wen, and G. Chen, "Privacy-Preserving Cloud Data Auditing Using Blockchain," Future Generation Computer Systems, vol. 109, pp. 153–162, 2020. DOI: 10.1016/j.future.2020.03.041