International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

Encrypted Digital Evidence Storage with Controlled Access Verification

Kandikonda Hemanth, Togiti Akhila*
Vaagdevi Engineering College, Warangal, 506005, Telangana, India.
*Correspondence: Togiti Akhila

ABSTRACT

The rapid growth of digital technologies, cloud computing, and online communication platforms has significantly increased the volume of digital evidence generated in domains such as cybercrime investigation, law enforcement, forensic analysis, and judicial proceedings. Traditional evidence management relied on physical media and manual verification processes, making evidence handling inefficient, time-consuming, and prone to human error. Although digital evidence management systems have improved storage and retrieval capabilities, many existing solutions still lack robust security mechanisms, fine-grained access control, reliable integrity verification, and comprehensive auditability. These limitations expose sensitive evidence to unauthorized access, data tampering, insider threats, and reduced legal admissibility. This work addresses the challenge of securely storing, managing, and preserving digital evidence within cloud-based environments, where distributed access increases security risks. The proposed framework is implemented as a Flask-based web application that integrates the Advanced Encryption Standard (AES) to ensure evidence confidentiality and the Secure Hash Algorithm (SHA-256) to verify data integrity and detect tampering. Role-Based Access Control (RBAC), request-driven authorization workflows, and detailed audit logging provide secure access management, accountability, and complete traceability throughout the evidence lifecycle. Additionally, a Lightning Memory-Mapped Database (LMDB) is employed to enable high-performance, transaction-consistent storage with efficient read and write operations. The framework delivers a secure, scalable, and efficient solution that enhances evidence confidentiality, integrity, forensic reliability, and overall operational performance in modern digital evidence management systems.

Key words: Digital Evidence Management, Digital Forensics, Role-Based Access Control, Data Integrity, Secure Cloud Storage, Flask Framework, Audit Logging

1. INTRODUCTION

In today's interconnected world, digital devices such as smartphones, wearables, and connected vehicles have become integral to daily life, continuously generating vast amounts of data. These mobile devices not only store extensive personal information but also remain portable and easily operable, creating a rich digital footprint that follows individuals wherever they go. The field of digital forensic sciences has emerged to leverage this data, enabling forensic investigators to uncover hidden truths in complex scenarios by analyzing information from suspects, victims, and other parties involved in a case. This capability has led to a significant increase in the use of digital evidence in civil and criminal proceedings in recent years [1]. The importance of digital evidence and the legitimacy of digital forensics are well established in legal contexts. For example, U.S. courts formally recognized digital information as admissible evidence and implemented the mandatory electronic discovery (eDiscovery) system in 2006, laying the foundation for modern digital forensics [2]. Over the past decade, digital evidence has played a critical role in solving major cases. In the Boston Marathon Bombing of 2013, digital forensic analysis of security footage and suspects' digital devices provided crucial investigative insights. Similarly, in the College Admissions Bribery Scandal of 2019, digital evidence including emails and text messages was instrumental in exposing fraudulent

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

activities. Despite its growing importance, the use of digital evidence presents unique challenges compared to traditional physical evidence, particularly with respect to admissibility in court. The massive volume of data and its rapid creation, duplication, and transmission make digital evidence highly susceptible to manipulation, alteration, or degradation. Several cases have highlighted the difficulties of maintaining the integrity and authenticity of digital evidence, resulting in its exclusion from legal proceedings [3].



Fig. 1.1: Digital Evidence

For instance, in Jones v. Riot Hospitality Group (2024), the District Court dismissed the lawsuit after determining that the plaintiff had intentionally deleted relevant text messages exchanged with co-workers, which were deemed critical evidence in the case [4]. Ensuring the integrity of digital evidence and the forensic investigation process, as well as establishing evidentiary admissibility, are fundamental challenges in digital forensics. The admissibility of evidence is governed by specific legal frameworks, such as the Federal Rules of Evidence in the United States. Rule 901, which addresses evidence authentication, requires proof that evidence is original and free from tampering.. In digital forensics, this requirement extends beyond demonstrating data integrity to verifying the legitimacy of the evidence source. This underscores the importance of originality and maintaining an unbroken investigative process. Chain of Custody (CoC) is a fundamental yet critical procedure that documents the complete and chronological handling of evidence. It ensures transparency in how digital evidence is collected, transferred, stored, and analyzed, thereby preserving its integrity and authenticity throughout the forensic investigation lifecycle [5].

- To ensure the secure storage of digital evidence by implementing AES-256 encryption for protecting data confidentiality.
- To implement Role-Based Access Control (RBAC) and authorization mechanisms that restrict evidence access exclusively to authorized users.
- To preserve the integrity and authenticity of digital evidence using SHA-256 hashing for effective tamper detection and verification.
- To maintain a transparent Chain of Custody (CoC) through comprehensive audit logging and activity tracking.
- To improve the efficiency and scalability of evidence storage using Lightning Memory-Mapped Database (LMDB) while ensuring transaction consistency and high-performance data access.

2. LITERATURE SURVEY

Inam Ul Mansoor, et al. [6] examined the relationship between the Chain of Custody (CoC) and digital forensics in ensuring the authenticity, integrity, and admissibility of digital evidence throughout forensic investigations. The study analysed existing legal frameworks, judicial precedents, and international standards governing the handling of electronic evidence while evaluating the role of emerging technologies such as blockchain and Artificial Intelligence (AI) in strengthening evidence management. It also identified vulnerabilities associated with evidence acquisition, storage, transfer, and preservation, emphasizing the need for standardized forensic procedures and harmonized legal practices to

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

improve evidentiary reliability across jurisdictions. Nath, et al. [7] investigated the significance of CoC as a fundamental component of digital forensic investigations by reviewing both its theoretical concepts and practical implementation strategies. The study categorized existing evidence management practices into Traditional Paper Trail, System-Oriented, and Infrastructure-Driven approaches and comparatively evaluated them based on evidence integrity, traceability, security, and operational efficiency. The analysis highlighted the strengths and limitations of each approach while emphasizing the importance of maintaining an unbroken and verifiable evidence trail throughout the forensic lifecycle. Wenqi Yan, et al. [8] proposed a secure digital evidence Chain of Custody protocol by integrating Revocable Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Boneh–Lynn–Shacham (BLS) digital signatures, and blockchain technology. The proposed protocol implemented fine-grained access control through attribute-based encryption while employing BLS signatures for digital evidence verification. Blockchain technology was incorporated to guarantee evidence integrity, immutability, and complete traceability, thereby providing a secure and transparent framework for digital evidence management. Mark Vella, et al. [9] proposed D-Cloud-Collector, a secure cloud forensic solution that utilized Hardware Security Modules (HSMs) to facilitate controlled live cloud forensic acquisition while maintaining tamper-evident access logs. A proof-of-concept implementation based on Google Drive and the SEcube hardware security module demonstrated that secure cloud evidence collection is feasible with acceptable performance overhead, enabling trustworthy acquisition of cloud-based digital evidence.

Deepti Rani, et al. [10] proposed a blockchain-based digital evidence management framework for smart Internet of Things (IoT) environments to ensure the confidentiality, integrity, authenticity, trustworthiness, and privacy of forensic evidence throughout the investigation process. The framework implemented user authentication before allowing evidence insertion or deletion and combined consortium blockchain technology with the InterPlanetary File System (IPFS) to provide decentralized, tamper-resistant, and secure storage of digital evidence. The proposed architecture significantly enhanced evidence traceability and strengthened Chain of Custody management within IoT forensic investigations. Sakshi, et al. [11] developed the Blockchain-based Digital Multimedia Evidence Preservation Framework for IoT (BEvPF-IoT) to securely preserve multimedia evidence generated by IoT devices. The proposed framework established a blockchain-enabled environment that prevented unauthorized modification or manipulation of digital evidence before its presentation in legal proceedings. By utilizing blockchain's immutability and decentralized architecture, the framework improved evidence authenticity, long-term preservation, and judicial admissibility. Reyana A., et al. [12] proposed an enhanced secure cloud storage and retrieval mechanism aimed at strengthening evidence integrity and access control in cloud-based forensic systems. The proposed approach incorporated optimized encryption, decryption, upload, and download mechanisms while improving cloud storage efficiency for digital evidence. Performance evaluation demonstrated that processing time increased proportionally with file size and format, while the enhanced retrieval mechanism significantly improved secure evidence management without compromising system performance.

Mohammad AlKhanafseh, et al. [13] proposed a secure and scalable framework for preserving digital evidence by integrating advanced Artificial Intelligence techniques into digital forensic investigations. The study employed a

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

Long Short-Term Memory (LSTM) autoencoder combined with linguistic steganography to securely generate coherent textual representations from binary data streams while maintaining high accuracy and low perplexity. The proposed framework contributed to secure evidence preservation and demonstrated the applicability of AI-based techniques for protecting sensitive forensic information. Munirah Maher Alshabibi, et al. [14] investigated the growing importance of cloud forensics as a specialized branch of digital forensics for investigating cyber incidents involving cloud computing environments. The study examined methodologies for identifying digital evidence, conducting forensic investigations, and presenting legally admissible findings to law enforcement agencies. Furthermore, the research emphasized that secure evidence acquisition, preservation, and analysis within cloud infrastructures are essential for combating modern cybercrime and ensuring the successful prosecution of digital offenses.

3. PROPOSED SYSTEM

This research methodology as shown in Fig. 1 follows a structured and security-centric approach for managing sensitive digital evidence in cloud-based environments by integrating cryptographic protection, controlled access verification, and audit-driven monitoring into a unified operational pipeline. The workflow begins with authenticated user interaction and secure evidence ingestion, after which data undergoes encryption prior to storage to preserve confidentiality. Role-based authorization and permission validation mechanisms ensure that only approved entities can access stored evidence, thereby preventing unauthorized usage. Cryptographic hashing techniques are employed to generate integrity fingerprints, enabling effective detection of tampering and preservation of authenticity. A lightweight and high-performance storage engine supports efficient management of encrypted data, permissions, and audit records. Continuous monitoring, detailed audit logging, and on-demand integrity verification further strengthen traceability, forensic reliability, and compliance throughout the entire evidence lifecycle.

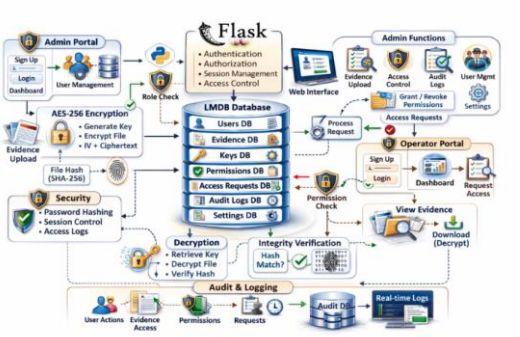


Fig. 1: System architecture of digital evidence storage.

User Authentication and Session Management: The workflow begins with user authentication, where administrators and operators log in through the web interface. Session management mechanisms validate user identity and enforce authorization rules based on assigned roles. This ensures that only authenticated users can interact with sensitive system functionalities.

Role-Based Access Control and Request Handling: Once authenticated, the system applies role-based access control to regulate permissible actions. Administrators can upload and manage evidence, while operators must submit access requests with proper justification. Each request is validated against authorization policies before further processing.

Evidence Upload and Cryptographic Protection: During evidence ingestion, uploaded files are securely processed by applying AES-256 encryption. Along with encryption, integrity fingerprints are generated to preserve authenticity. This step ensures that sensitive data is protected before being stored in the backend repository.

Secure Storage and Metadata Management: Encrypted evidence, associated metadata, and

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

audit information are stored using a lightweight LMDB-based storage engine. The storage mechanism supports fast access while maintaining transaction consistency. Separation of encrypted data and access records strengthens overall data security.

Controlled Evidence Access and Decryption: When access is approved, the system retrieves encrypted evidence and performs in-memory decryption. This approach prevents exposure of plaintext data on disk while allowing authorized viewing or download. Access activities are tracked to maintain accountability.

Integrity Verification and Audit Logging: Throughout the lifecycle, all operations such as uploads, access requests, downloads, and verification checks are logged. Integrity verification can be performed at any time to detect tampering. This continuous auditing ensures traceability, forensic reliability, and compliance.

4. RESULTS ANALYSIS

Fig. 2 depicts the secure evidence upload interface used by administrators to add new digital assets into the system. The screen illustrates the process of selecting files, assigning metadata such as case numbers and descriptions, and initiating encryption during upload. It represents the implementation of secure storage practices where files are encrypted before being saved to maintain confidentiality. The upload workflow ensures only supported file types are accepted and associates each file with unique identifiers.

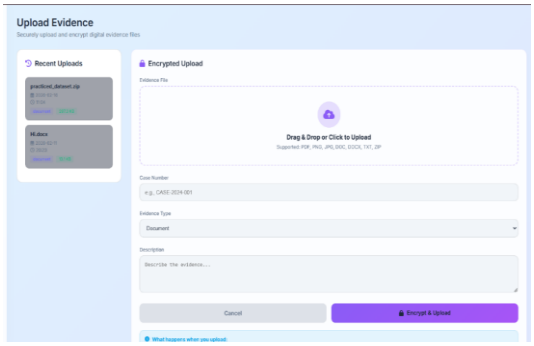


Fig. 2: Upload Evidence Screen

Fig. 3 illustrates the access control management interface where administrators handle operator permissions and access requests. The screen depicts pending requests and permission assignments, demonstrating the role-based authorization model implemented within the system. It represents how administrators review requests, grant or revoke permissions, and maintain controlled access to sensitive evidence. The interface supports centralized permission management to ensure that only authorized users can view or download specific files.

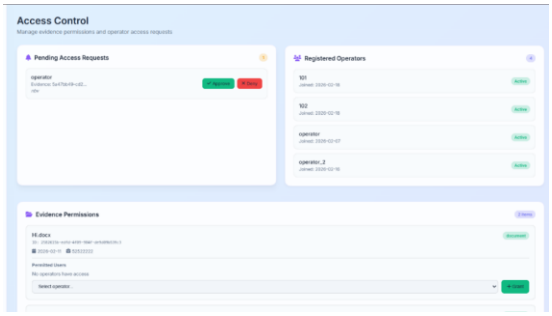


Fig. 3: Access Control Screen

Fig. 4 depicts the audit logs interface that records and displays system activities for monitoring and traceability. The screen illustrates chronological tracking of user actions such as login, upload, verification, and access control events. It represents the implementation of an audit trail mechanism that ensures transparency and accountability within the platform. The logs enable administrators to review historical activities and detect potential security issues or unauthorized behavior.

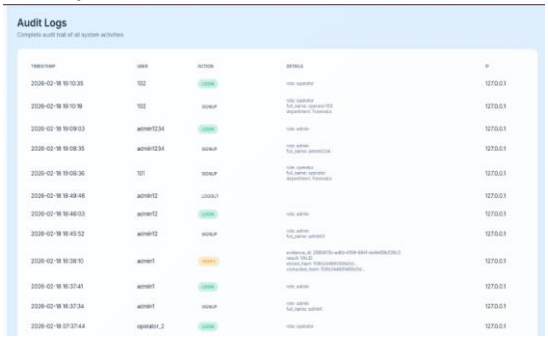


Fig. 4: Audit Logs Screen

Received: 30-05-2026 | Accepted: 01-07-2026 | Published: 08-07-2026

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

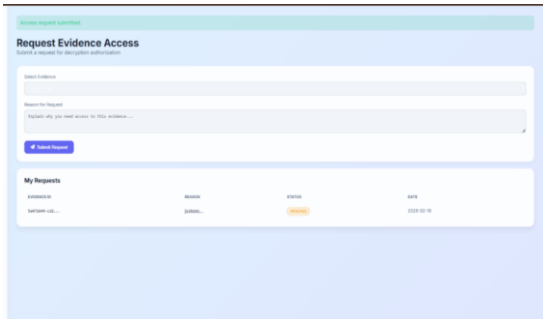


Fig. 5: Requesting Evidence Access Screen

Fig. 5 depicts the evidence access request module used by operators to submit authorization requests for restricted files. The screen illustrates structured request submission including evidence selection and justification details required for administrative approval. It represents the workflow of controlled access where requests are reviewed before granting permissions. The interface also displays previously submitted requests along with their status, supporting transparency and tracking.

Conclusion

This research successfully develops a secure and efficient digital evidence management framework that addresses the major challenges of confidentiality, integrity, and controlled access in cloud-based forensic environments. The proposed system integrates AES encryption to safeguard sensitive digital evidence from unauthorized access and SHA-256 hashing to verify data integrity and detect any unauthorized modifications. A Role-Based Access Control (RBAC) mechanism, combined with a structured request–approval workflow, ensures that evidence is accessed only by authorized users, thereby strengthening security and accountability throughout the evidence lifecycle. To improve storage efficiency and system performance, the framework utilizes Lightning Memory-Mapped Database (LMDB), which provides fast, transaction-consistent read and write operations while minimizing storage overhead. The implementation of in-memory decryption further enhances security by limiting plaintext exposure and enabling faster evidence retrieval for authorized users. Additionally, comprehensive audit logging maintains a complete Chain of Custody by recording all evidence-related activities, thereby improving traceability and supporting forensic investigations with minimal performance overhead. The modular Flask-based architecture ensures scalability, maintainability, and efficient request processing, making the framework suitable for modern digital forensic applications. This study delivers a reliable, secure, and high-performance solution that preserves evidence authenticity, strengthens forensic reliability, and supports the secure management of digital evidence in contemporary cloud-based environments.

REFERENCES

[1] "Hacking cases with digital forensics," 2018. Available online: https://www.tutorialspoint.com/hacking/hacking_cases_with_digital_forensics.htm. Accessed August 21, 2023.

[2] Al-Khateeb, H., Epiphaniou, G., and Daly, H., "Blockchain for modern digital forensics: The chain of custody as a distributed ledger," in Blockchain and Clinical Trial: Securing Patient Data,pp. 149–168, 2019.

[3] "In Boston bombing, flood of digital evidence is a blessing and a curse," CNN, 2013. Available online: https://www.cnn.com/2013/04/17/tech/mobile/boston-bombing-evidence-search-verge/index.html.Accessed October 4, 2023.

[4] "The college admissions scandal that shook higher education," BestColleges, 2023. Available online: https://www.bestcolleges.com/blog/operation-varsity-blues-college-admissions-scandal/. Accessed October 4, 2023.

[5] "Legal lessons learned: Five times digital evidence was denied in court," Pagefreezer Blog, 2017. Available online:

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

https://blog.pagefreezer.com/legal-lessons-learned-5-times-digital-evidence-was-denied-in-court.Accessed August 21, 2023

[6] Inam Ul Mansoor, Sheikh & Shah, Shaeyuq & Wani, Showkat Ahmad. (2025). Digital Forensics and Chain of Custody: Safeguarding the Integrity and Admissibility of Electronic Evidence in Legal Proceedings. 10.4018/979-8-3373-3023-5.ch008.

[7] Nath, Souradip & Summers, Keb & Baek, Jaejong & Ahn, Gail-Joon. (2024). Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics. 10.1109/TPS-ISA62245.2024.00012.

[8] Wenqi Yan, Jiachen Shen, Zhenfu Cao, and Xiaolei Dong. 2020. Blockchain Based Digital Evidence Chain of Custody. In Proceedings of the 2020 2nd International Conference on Blockchain Technology (ICBCT '20). Association for Computing Machinery, New York, NY, USA, 19–23. https://doi.org/10.1145/3390566.3391690

[9] Vella, M., Colombo, C. (2022). D-Cloud-Collector: Admissible Forensic Evidence from Mobile Cloud Storage. In: Meng, W., Fischer-Hübner, S., Jensen, C.D. (eds) ICT Systems Security and Privacy Protection. SEC 2022. IFIP Advances in Information and Communication Technology, vol 648. Springer, Cham. https://doi.org/10.1007/978-3-031-06975-8_10

[10] Rani, D., Gill, N.S., Gulia, P. et al. A secure digital evidence preservation system for an iot-enabled smart environment using ipfs, blockchain, and smart contracts. Peer-to-Peer Netw. Appl. 18, 5 (2025). https://doi.org/10.1007/s12083-024-01855-z

[11] Sakshi, Aruna Malik, Ajay K. Sharma, Blockchain-based digital chain of custody multimedia evidence preservation framework for internet-of-things, Journal of Information Security and Applications, Volume 77, 2023, 103579, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2023.103579.

[12] A, R.; Kautish, S.; Juneja, S.; Mohiuddin, K.; Karim, F.K.; Elmannai, H.; Ghorashi, S.; Hamid, Y. Enhanced Cloud Storage Encryption Standard for Security in Distributed Environments. Electronics 2023, 12, 714. https://doi.org/10.3390/electronics12030714

[13] AlKhanafseh, M.; Surakhi, O. Evidence Preservation in Digital Forensics: An Approach Using Blockchain and LSTM-Based Steganography. Electronics 2024, 13, 3729. https://doi.org/10.3390/electronics13183729

[14] Alshabibi, M.M.; Bu dookhi, A.K.; Hafizur Rahman, M.M. Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review. Computers 2024, 13, 213. https://doi.org/10.3390/computers13080213