iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78170

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Mobile Evidence Preservation Using Blockchain And IPFS: A Conceptual Review

K Madhusha[1], Anunanda V K[2], Abhina K[3], Aarya M S[4], Ms. Athira Balachandran[5]
[1, 2, 3, 4]*Department of Computer Science and Engineering (CSE), Sree Narayana Guru College of Engineering and Technology Korom, Payyanur, Kannur*
[5]*Assistant Professor, Department of Computer Science and Engineering (CSE), Sree Narayana Guru College of Engineering and Technology Korom, Payyanur, Kannur*

Abstract: ***Digital evidence plays a crucial role in modern criminal investigations, cybercrime analysis, and legal proceedings. However, conventional evidence storage systems suffer from vulnerabilities such as unauthorized access, data tampering, centralized failures, and lack of transparency. With the increasing use of mobile devices for capturing evidence such as images, videos, audio recordings, and documents, ensuring the integrity and authenticity of such evidence has become a significant challenge.This paper presents a conceptual review of a mobile-based evidence preservation model that integrates Blockchain technology and the InterPlanetary File System (IPFS) to provide a secure, tamper-resistant, and decentralized framework. Blockchain is used for immutable hash storage and traceability, while IPFS enables efficient and distributed storage of large digital evidence files. The proposed model highlights the architecture, working principles, roles of stakeholders, and advantages over traditional systems.***

I. INTRODUCTION

The rapid growth of smartphones and digital media has transformed the way evidence is captured and stored. Mobile devices are often the first source of evidence in cases involving cybercrime, harassment, accidents, or illegal activities. However, digital evidence is highly susceptible to modification, deletion, and unauthorized access, which raises serious concerns regarding its admissibility in courts of law.

Traditional centralized evidence management systems depend heavily on trusted third parties and centralized servers, making them vulnerable to single points of failure, insider attacks, and data manipulation. Establishing a reliable chain of custody remains a major challenge in such systems.

Blockchain technology offers immutability, transparency, and decentralized trust, making it a promising solution for evidence preservation. When combined with IPFS, which provides efficient decentralized storage, a scalable and secure evidence management framework can be achieved. This paper conceptually explores such a system designed as both a mobile application and web platform**.**

II. RELATED WORK

Existing research has explored blockchain-based frameworks for digital forensics to ensure data integrity and chain-of-custody management. Several approaches utilize blockchain to store forensic logs and verification records, enhancing transparency and accountability.

However, direct storage of large multimedia files on blockchain platforms is inefficient due to storage and cost constraints.IPFS has been proposed as a complementary solution for decentralized file storage, enabling content-addressable data retrieval using cryptographic hashes.

Recent studies recommend a hybrid approach where blockchain stores metadata and IPFS hash values, while the actual evidence is maintained off-chain. Despite these advancements, limited research focuses on mobile-centric evidence capture with role-based administrative control**,** which the proposed conceptual model aims to address.

III. LITERATURE REVIEW

1) Blockchain-based Privacy Preservation Technique for Digital Forensics Records

The paper **"**Blockchain-based Privacy Preservation Technique for Digital Forensics Records" proposes the use of blockchain technology combined with cryptographic mechanisms to ensure secure storage and privacy of digital forensic records.

©IJRASET: All Rights are Reserved

The study highlights how immutability and distributed ledger properties can prevent unauthorized modification of forensic data. However, the approach mainly concentrates on record preservation after evidence collection and does not describe a complete evidence lifecycle, such as real-time acquisition, verification, and large-scale storage handling. Practical implementation aspects, especially storage efficiency and usability for investigators, are not deeply addressed.

2) A Metamodeling Approach for IoT Forensic

The work **"**A Metamodeling Approach for IoT Forensic**"** focuses on organizing and structuring the investigation process in complex IoT environments.

By defining a metamodel, the paper aims to standardize evidence identification and forensic workflows in heterogeneous IoT systems.

Although this improves conceptual understanding and investigation consistency, the model lacks a robust security mechanism for preserving collected evidence. The absence of immutable storage and automated tamper detection reduces its reliability in legal and court-admissible forensic scenarios.

3) A Novel Administration Model for Managing and Organising the Heterogeneous Information Security Policy Field

In **"**A Novel Administration Model for Managing and Organising the Heterogeneous Information Security Policy Field**",** the authors address challenges related to managing diverse security policies within organizations.

The paper contributes at an administrative and policy level by proposing systematic control and organization of security information.

While useful for governance, this approach does not directly tackle forensic evidence preservation, chain of custody, or protection against evidence tampering, making it less applicable for practical digital forensic investigations

4) Blockchain Technology as a Strategic Weapon to Bring Procurement 4.0 Truly Alive

The study **"**Blockchain Technology as a Strategic Weapon to Bring Procurement 4.0 Truly Alive**"** provides a broad literature review discussing blockchain's role in enhancing transparency, trust, and automation in modern digital systems.

The paper is largely theoretical and strategic, focusing on future research directions rather than domain-specific solutions. Although it reinforces the relevance of blockchain technology, it does not offer a concrete forensic framework or an operational model for managing digital evidence.

5) Blockchain-Based Digital Forensic Evidence Management Chain of Custody

Another related work, **"**Blockchain-Based Digital Forensic Evidence Management Chain of Custody**",** focuses specifically on maintaining a secure chain of custody using blockchain.

While it successfully demonstrates how blockchain can ensure tamper-proof custody records, the approach often assumes centralized storage and does not incorporate efficient off-chain storage solutions. This limits scalability when dealing with large multimedia evidence files such as images, videos, and audio data.

IV. CONCLUSION FROM LITERATURE REVIEW

From the reviewed literature, it is evident that most existing works either focus on theoretical frameworks, policy-level management, or partial forensic solutions. While blockchain is widely recognized for ensuring integrity and immutability, many studies do not address practical challenges such as scalable storage, real-time evidence upload, and ease of use for investigators. Additionally, several approaches lack a complete end-to-end system covering evidence acquisition, verification, storage, and tamper detection.

The proposed project is therefore chosen as it provides a comprehensive and implementable digital evidence preservation system by integrating blockchain with IPFS for efficient off-chain storage. Unlike existing studies, the project supports both mobile and web platforms, enabling real-time evidence collection and verification. The use of hash comparison for tamper detection and separate admin and user portals ensures transparency, accountability, and legal reliability. By overcoming the limitations observed in prior literature, the proposed system offers a scalable, secure, and practical solution, making it more suitable for real-world digital forensic applications.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

V. PROPOSED SYSTEM ARCHITECTURE

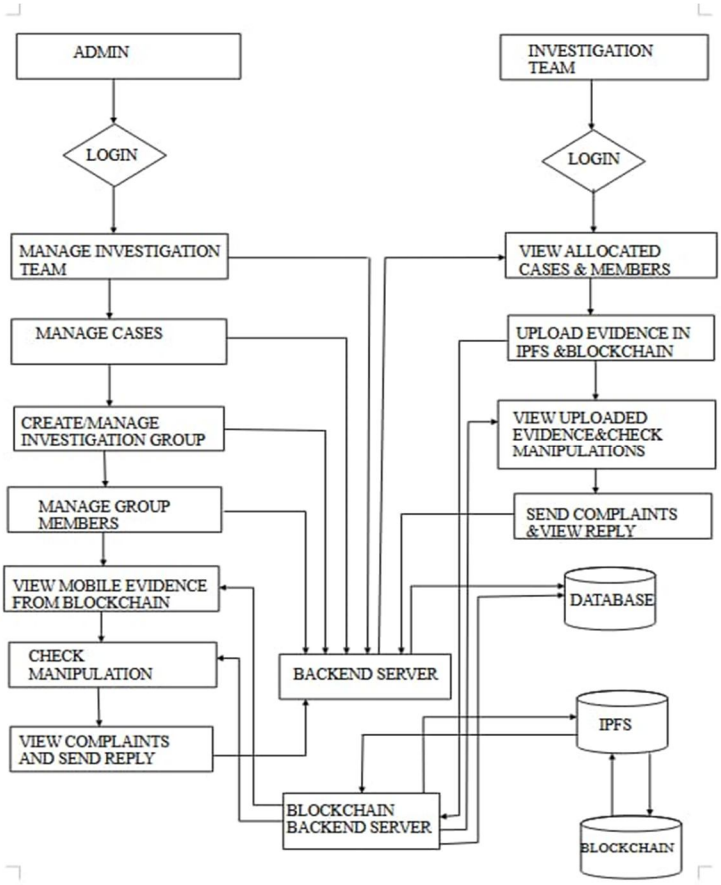


Fig. 1 Proposed System Architecture of Mobile Evidence Preservation System

The overall architecture of the proposed system is shown in Fig. 1. The system consists of two primary user roles: Admin and Investigation Team. The investigation team captures and uploads digital evidence through the system, which is securely stored using IPFS while the corresponding hash and metadata are recorded on the blockchain. The backend server coordinates communication between the user interfaces, blockchain backend, and storage components. The admin module manages cases, investigation groups, and verification of evidence integrity, ensuring transparency and tamper detection throughout the evidence lifecycle.
The proposed system consists of three primary components:

A. Mobile Application Module

The mobile application enables authorized users to capture and upload digital evidence such as images, videos, and documents. Upon capture, a cryptographic hash is generated, and the data is uploaded to IPFS, ensuring content-based addressing.

B. Blockchain Network

The blockchain layer stores:

1) IPFS hash of the evidence
2) Timestamp of submission
3) Evidence identifier
4) User and transaction metadata

Due to blockchain immutability, any attempt to tamper with the evidence results in a hash mismatch, indicating unauthorized modification.

C. Web-Based Admin Portal

The administrator portal provides functionalities such as:

1) Evidence verification
2) User and role management
3) Audit trail monitoring
4) Integrity validation

This role-based access structure ensures controlled and transparent evidence handling.

VI. WORKING METHODOLOGY

The working methodology of the proposed mobile evidence preservation system is designed to ensure integrity, authenticity, transparency, and accountability throughout the lifecycle of digital evidence. The methodology follows a structured sequence of processes that collectively maintain a reliable chain of custody from the moment of evidence capture to verification.

A. Evidence Acquisition

The process begins with evidence acquisition using a mobile device. Evidence may include images, videos, audio recordings, or documents captured during an incident. At this stage, the system ensures that the
evidence is collected in its original form without introducing modifications. The captured evidence is treated as a digital artifact whose integrity must be preserved from the point of origin.

B. Cryptographic Hash Generation

Once the evidence is acquired, a cryptographic hash value is generated. Hashing is a one-way mathematical process that converts input data into a fixed-length output known as a hash digest. This hash acts as a unique digital fingerprint of the evidence. Even the smallest modification in the evidence file results in a completely different hash value, making hashing a reliable mechanism for integrity verification.

C. Decentralized Storage Using IPFS

The digital evidence is then stored in the InterPlanetary File System (IPFS), a peer-to-peer distributed storage network. Instead of using location-based addressing, IPFS employs content-based addressing, where files are retrieved using their cryptographic hash. As a result, any attempt to modify the evidence leads to the generation of a different content identifier, immediately revealing unauthorized alterations. This approach ensures efficient storage and eliminates dependency on centralized servers.

D. Immutable Record Creation on Blockchain

After the evidence is successfully stored in IPFS, its corresponding content identifier, along with metadata such as timestamp and evidence details, is recorded on the blockchain. Blockchain functions as an immutable ledger where each transaction is permanently recorded and verified through consensus mechanisms. Since blockchain records cannot be altered retrospectively, this step guarantees that the integrity-related metadata remains tamper-proof throughout the evidence lifecycle.

E. Chain of Custody Maintenance

Maintaining an unbroken chain of custody is critical for legal admissibility. In the proposed methodology, blockchain records serve as transparent custody logs, documenting when the evidence was submitted and verified. Each entry establishes accountability and provides a verifiable history of evidence handling without relying on centralized authorities.

F. Evidence Verification Process

During evidence access or verification, the stored evidence file is retrieved from IPFS, and a new hash is computed. This hash is compared with the original hash stored on the blockchain. If both values match, the evidence is confirmed to be authentic and unaltered. Any mismatch indicates potential tampering, thereby protecting the system from forged or manipulated evidence.

G. Access Control and Auditability

To prevent unauthorized access, the system incorporates role-based access control through an administrative framework. Authorized personnel can view or verify evidence while all actions remain auditable. Blockchain transparency ensures that verification activities are traceable, further enhancing system accounability.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

H. Summary of Methodology Significance

The proposed working methodology theoretically demonstrates how blockchain and IPFS complement each other to preserve evidence integrity. Blockchain ensures immutability and traceability, while IPFS provides scalable and decentralized storage. Together, they establish a trustworthy and tamper-evident framework suitable for mobile-based digital evidence preservation.

VII. CONCLUSION

Digital forensic investigations increasingly require secure and trustworthy mechanisms to preserve the integrity of digital evidence. Traditional centralized systems are vulnerable to tampering, unauthorized access, and lack transparent chain-of-custody management. To address these challenges, this project proposes a blockchain-based digital evidence preservation model that ensures immutability, authenticity, and traceability of forensic data.

By integrating blockchain with IPFS-based off-chain storage, the system efficiently handles large multimedia evidence while maintaining tamper detection through cryptographic hash verification. The mobile and web-based implementation supports real-time evidence collection and role-based access through user and administrator portals. Overall, the proposed approach provides a scalable, secure, and practical solution that enhances the reliability and legal admissibility of digital forensic evidence.

REFERENCES

[1] S. Durga, E. Daniel, S. Deepakanmani, T. Mary Neeba, and V. Ravi, “Blockchain-based Privacy Preservation Technique for Digital Forensics Records,” in Artificial Intelligence and Blockchain in Digital Forensics, Springer Nature, Cham, 2022.

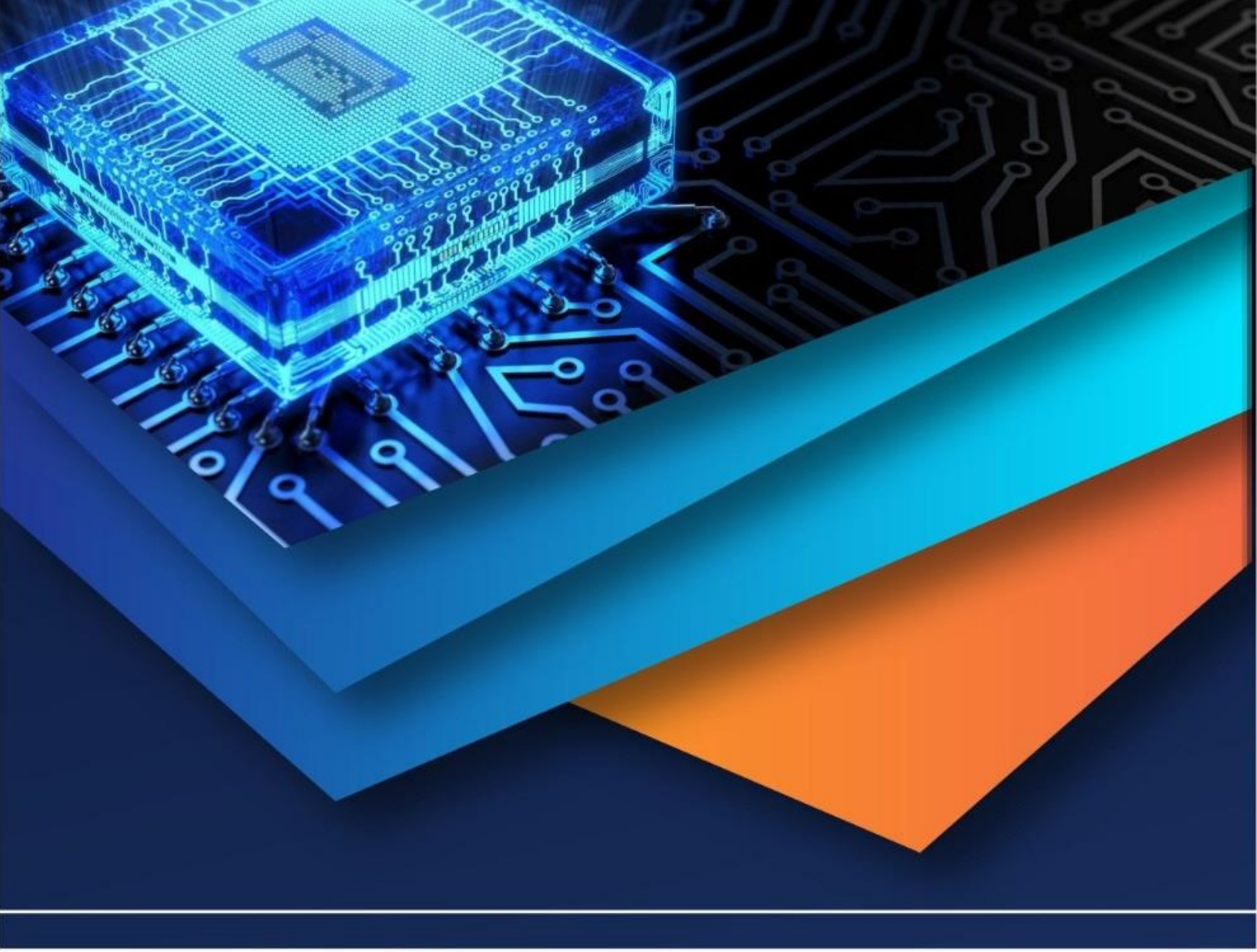
[2] N. Xiao, Z. Wang, X. Sun, and J. Miao, “A Novel Blockchain-based Digital Forensics Framework for Preserving Evidence and Enabling Investigation in Industrial Internet of Things,” Alexandria Engineering Journal, vol. 86, pp. 631–643, Jan. 2024.

[3] A. H. Lone and R. N. Mir, “Forensic-Chain: Blockchain-based Digital Forensics Chain of Custody with PoC in Hyperledger Composer,” Digital Investigation, vol. 28, pp. 44–55, Mar. 2019.

[4] M. I. Shrunga, A. Ashwini, U. Deepthi, R. Spandana, and K. Rakesh, “A Survey on Blockchain Based Digital Forensics Framework,” International Journal for Research in Applied Science & Engineering Technology, vol. 12, no. IV, Apr. 2024.

[5] S. Kumar and A. Saha, “Internet-of-Forensics: A Blockchain-based Digital Forensics Framework for IoT Applications,” Future Generation Computer Systems, vol. 120, pp. 13–25, 2021.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)