International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Security Enhancement of Forensic Evidences Using Blockchain

Jerrin John[1], Sindhu Daniel[2]

[1]Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India
Email: *Jerryjohn7676[at]gmail.com*

[2]Professor, Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India

Abstract: ***The integrity, authenticity, and confidentiality of forensic evidence are critical factors in modern criminal investigations and judicial proceedings. Traditional evidence management systems often rely on centralized storage and manual handling processes, which are vulnerable to tampering, unauthorized access, data loss, and chain-of-custody violations. These limitations can compromise the reliability of evidence and weaken legal outcomes. To address these challenges, this study proposes a blockchain-based framework for enhancing the security of forensic evidence management systems. Blockchain technology, a decentralized and immutable distributed ledger, offers a robust solution for ensuring transparency and trust in evidence handling. In the proposed system, forensic evidence is digitally recorded and its cryptographic hash is stored on the blockchain, ensuring that any alteration in the original data can be easily detected. Each transaction related to the evidence such as collection, transfer, analysis, and storage is logged as a time-stamped block, creating a tamper-proof and verifiable chain of custody. Smart contracts are integrated into the system to automate access control, ensuring that only authorized personnel can interact with the evidence under predefined conditions. Additionally, encryption techniques are employed to protect sensitive information, while decentralized storage solutions are used to securely store large forensic files off-chain, maintaining efficiency and scalability. The system also enables real-time tracking and auditing of evidence, thereby enhancing accountability among law enforcement agencies and forensic experts. This approach significantly reduces the risks associated with evidence manipulation, data breaches, and human errors. By providing a transparent, secure, and auditable platform, blockchain technology strengthens the credibility of forensic evidence in legal proceedings. The proposed model demonstrates improved reliability, enhanced data integrity, and increased trust among stakeholders, including investigators, legal authorities, and judicial systems. Overall, the integration of blockchain in forensic evidence management presents a transformative solution to modern digital forensics challenges, paving the way for more secure and efficient criminal justice processes.***

Keywords: Blockchain Technology, Digital Forensics, Forensic Evidence Management, Chain of Custody, Data Integrity, Evidence Authentication, Cryptographic Hashing, Smart Contracts, Decentralized Storage, Tamper-Proof Systems, Cybersecurity, Distributed Ledger, Secure Data Sharing, Access Control, Evidence Tracking, Immutable Records, Audit Trail, Data Privacy.

1. Introduction

In the modern digital era, the role of forensic evidence has become increasingly significant in criminal investigations and judicial processes. With the rapid growth of cyber crime, digital fraud, and technologically sophisticated offenses, the volume and complexity of forensic evidence have expanded considerably. Digital forensic evidence including files, images, logs, and communication records must be handled with extreme care to ensure its integrity, authenticity, and admissibility in courts of law. However, traditional forensic evidence management systems face several critical challenges, including data tampering, lack of transparency, unauthorized access, and inefficient chain-of-custody tracking.

Conventional systems typically rely on centralized databases and manual documentation processes to manage evidence. These approaches are inherently vulnerable to single points of failure, insider threats, and cyber attacks. Moreover, maintaining a reliable chain of custody documenting every stage of evidence collection, transfer, storage, and analysis is often prone to human error and manipulation. Any compromise in this process can lead to the rejection of evidence in legal proceedings, thereby affecting the outcome of justice.

To overcome these limitations, emerging technologies such as blockchain offer a promising solution for enhancing the security and reliability of forensic evidence management. Blockchain is a decentralized and distributed ledger technology that ensures immutability, transparency, and traceability of data. Once information is recorded on a blockchain, it cannot be altered or deleted without consensus from the network, making it highly resistant to tampering. This characteristic is particularly valuable in forensic applications, where maintaining the originality and credibility of evidence is paramount.

In a blockchain based forensic system, each piece of evidence is associated with a unique cryptographic hash that acts as its digital fingerprint. Instead of storing large evidence files directly on the blockchain, which may be inefficient, the system stores these hashes along with metadata such as timestamps, ownership details, and transaction records. Any change in the original evidence would result in a mismatch of the hash value, thereby immediately indicating tampering. Additionally, every interaction with the evidence is recorded as a transaction on the blockchain, creating a permanent and verifiable audit trail.

The integration of smart contracts further enhances the system by automating access control and evidence handling procedures. Smart contracts enforce predefined rules, ensuring that only authorized individuals can access or modify evidence under specific conditions. This reduces the risk of unauthorized access and minimizes human intervention, thereby improving operational efficiency.

Furthermore, encryption mechanisms and decentralized storage solutions are employed to secure sensitive data while maintaining scalability and performance.

The adoption of blockchain technology in forensic evidence management not only improves data security but also increases transparency and trust among stakeholders, including law enforcement agencies, forensic experts, and judicial authorities. It provides a reliable framework for real-time tracking, auditing, and verification of evidence, thereby strengthening the overall criminal justice system.

In conclusion, the application of blockchain technology addresses the key challenges associated with traditional forensic evidence management systems. By ensuring data integrity, enhancing chain-of-custody tracking, and providing a tamper-proof environment, blockchain presents a transformative approach to securing forensic evidence in the digital age.

2. Objectives

To design and develop a secure, transparent, and tamper-proof forensic evidence management system using blockchain technology that ensures data integrity, authenticity, and reliable chain-of-custody tracking.

The specific objectives of the proposed system are as follows:

- Implement cryptographic hashing techniques to generate a unique digital fingerprint for each piece of evidence.
- Detect any unauthorized modification by comparing hash values over time.
- Prevent data tampering by storing hash records on an immutable blockchain ledger.
- Record every action (collection, transfer, analysis, storage) as a blockchain transaction.
- Provide time-stamped and verifiable logs for all evidence-related activities.
- Eliminate manual errors and ensure accountability throughout the evidence lifecycle.
- Enable real-time tracking of forensic evidence across different stakeholders.
- Allow authorized users to verify the history and origin of evidence.
- Build trust among investigators, forensic experts, and legal authorities.
- Use smart contracts to define and enforce role-based access permissions.
- Restrict unauthorized access to sensitive forensic data.
- Automate validation processes for evidence handling operations.
- Apply encryption techniques to safeguard evidence data from breaches.
- Store large forensic files securely using off-chain or decentralized storage systems.
- Ensure only authorized entities can decrypt and access the original data.
- Provide mechanisms to verify the originality and authenticity of evidence.
- Enable quick validation using blockchain-stored hashes.
- Support legal admissibility by ensuring credibility and reliability.
- Eliminate single points of failure through decentralization.
- Minimize risks associated with centralized databases.
- Provide secure audit logs that cannot be altered by insiders.
- Utilize smart contracts to automate workflows such as evidence submission and approval.
- Reduce manual intervention and administrative overhead.
- Improve operational efficiency in forensic investigations.
- Integrate blockchain with off-chain storage systems (e.g. IPFS or cloud storage).
- Ensure efficient handling of large multimedia forensic files.
- Maintain system performance while preserving security.
- Ensure compliance with legal standards for evidence handling.
- Provide immutable audit trails for courtroom verification.
- Increase confidence in digital forensic processes among judicial authorities.

3. Existing System

The existing system for managing forensic evidence largely relies on centralized digital databases and traditional chain-of-custody procedures, which are vulnerable to manipulation, data breaches, and unauthorized access. In conventional forensic frameworks, evidence collected from crime scenes is stored in secure physical repositories and documented using manual logs or centralized digital systems.

While these methods aim to maintain integrity, they often suffer from issues such as lack of transparency, single points of failure, delayed verification, and susceptibility to insider threats. Digital evidence, in particular, faces challenges related to tampering, duplication, and difficulties in proving authenticity during legal proceedings.

The absence of a robust, immutable audit trail makes it difficult to track every interaction with the evidence, thereby weakening trust among stakeholders such as investigators, legal authorities, and forensic experts. Moreover, current systems often depend on third-party intermediaries for validation and verification, increasing the risk of errors and inefficiencies.

Without the integration of advanced technologies like blockchain, the existing infrastructure struggles to ensure real-time traceability, secure data sharing, and non-repudiation of forensic evidence, ultimately limiting the reliability and admissibility of evidence in court.

4. Proposed System

The proposed system is designed to overcome the limitations of traditional forensic evidence management systems by integrating security, transparency, automation, and real-time traceability into a unified platform using Blockchain Technology. The system ensures both secure local handling of evidence and globally verifiable records, thereby significantly enhancing the integrity, reliability, and admissibility of forensic data.

The system consists of several key components, including a secure evidence acquisition module, a blockchain network for decentralized storage, a hashing mechanism based on Cryptographic Hashing, and access control mechanisms

implemented using Smart Contracts. Additionally, a cloud-based interface is integrated for real-time monitoring, tracking, and visualization of forensic evidence records.

When forensic evidence is collected, whether digital or physical, it is first digitized and processed through the hashing module, which generates a unique hash value representing the integrity of the evidence. This hash, along with metadata such as timestamp, location, and investigator details, is recorded on the blockchain network. The decentralized ledger ensures that once the data is stored, it cannot be altered or deleted, thus maintaining a tamper-proof chain of custody.

The system continuously tracks all interactions with the evidence. Whenever evidence is accessed, transferred, or analyzed, a new transaction is recorded on the blockchain. The smart contract automatically verifies permissions and logs the activity, ensuring that only authorized personnel can interact with the evidence. If any unauthorized attempt or inconsistency is detected, the system immediately flags it, maintaining strict accountability.

In addition, the system provides real-time updates to authorized users through a web or mobile interface, allowing investigators, forensic experts, and legal authorities to monitor evidence status remotely. The integration with cloud platforms enables efficient data visualization and easy retrieval of historical records for auditing and legal purposes.

This integrated approach ensures secure evidence handling, automated verification, transparent tracking, and reliable data sharing. By eliminating single points of failure and preventing tampering, the proposed system significantly enhances the trustworthiness and effectiveness of forensic evidence management in modern investigative environments.

5. Methodology

The proposed system follows a continuous monitoring and event-driven methodology to ensure secure handling, verification, and traceability of forensic evidence using Blockchain Technology. The system operates by continuously tracking evidence related activities and initiating automated validation and recording processes whenever any interaction with the evidence occurs.

When forensic evidence is collected, it is first digitized (if physical) and processed through a hashing mechanism based on Cryptographic Hashing. This process generates a unique hash value representing the original state of the evidence. The generated hash, along with essential metadata such as timestamp, case ID, location, and investigator credentials, is recorded on the blockchain network. This ensures that the initial state of the evidence is permanently secured and cannot be altered.

Under normal conditions, when no modifications or access requests are made, the system continuously maintains and monitors the stored records across the distributed ledger. Authorized users can view evidence details through a secure interface, while periodic synchronization ensures consistency across all nodes in the blockchain network.

Whenever an event occurs such as evidence access, transfer, analysis, or update the system triggers an automated response. A new transaction is generated and added to the blockchain, recording the action along with updated metadata. The integrity of the evidence is verified by recalculating and comparing hash values to detect any unauthorized changes. If the computed hash differs from the original, the system immediately flags the discrepancy, ensuring tamper detection.

Access control and authorization are managed using Smart Contracts, which automatically enforce predefined rules. Only authorized personnel are allowed to interact with the evidence, and every action is transparently logged. In case of unauthorized access attempts, the system generates alerts and restricts further interaction.

Additionally, all evidence related activities are available for real-time monitoring through a web or mobile interface. Investigators, forensic experts, and legal authorities can remotely access up-to-date information, verify the chain of custody, and audit historical records without compromising security.

This layered methodology ensures continuous monitoring, automated validation, tamper detection, secure access control, and transparent record-keeping. By integrating blockchain into forensic workflows, the system significantly enhances evidence integrity, accountability, and trustworthiness in digital forensic investigations.

6. System Architecture

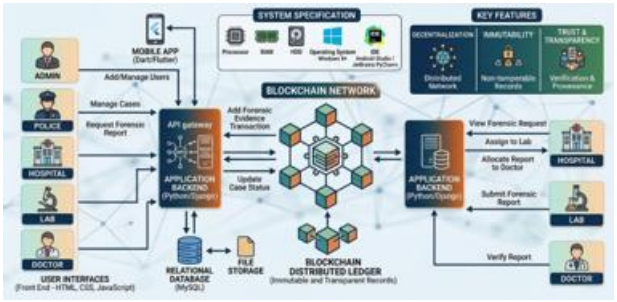

Figure 1: System architecture of the forensic evidence security enhancement using blockchain

The block diagram illustrates the overall architecture of the proposed blockchain-based forensic evidence security system. The system begins with evidence acquisition sources, such as digital devices, forensic tools, and investigators, which collect forensic evidence in various formats (images, documents, logs, videos, etc.).

Once the evidence is collected, it is passed to the Evidence Processing Module, where the data is preprocessed and converted into a standardized format. A cryptographic hash (e.g., SHA-256) is generated for each piece of evidence to ensure integrity and uniqueness.

The generated hash, along with metadata such as timestamp, case ID, and investigator details, is then sent to the Blockchain Network. The blockchain acts as a decentralized and tamper-proof ledger where all evidence records are

securely stored as transactions. Smart contracts are used to enforce access control, validate evidence submission, and maintain the chain of custody.

If any modification is attempted on the evidence, the system detects it by recalculating the hash and comparing it with the stored hash on the blockchain. This ensures data integrity and authenticity.

The Storage Module (off-chain storage such as cloud or IPFS) stores the actual forensic files, while only the hash and metadata are stored on the blockchain to improve efficiency and scalability.

The system includes a User Interface Module, which allows authorized users such as investigators, forensic experts, and legal authorities to upload, verify, and access evidence securely. Authentication mechanisms ensure that only authorized personnel can interact with the system.

Additionally, a Notification Module alerts users in case of unauthorized access attempts or evidence tampering. The system may also provide real-time updates and logs for auditing purposes.

Overall, the integration of blockchain technology ensures secure storage, transparency, immutability, and traceability of forensic evidence throughout its lifecycle.

7. Result & Discussion

The evaluation of the Security Enhancement of Forensic Evidences Using Blockchain system against traditional forensic evidence management methods highlights several significant advantages in terms of security, transparency, and reliability. In conventional systems, forensic evidence is often stored in centralized databases or physical records, making it vulnerable to tampering, unauthorized access, and loss of data. Additionally, tracking the chain of custody across multiple departments such as police stations, hospitals, and forensic labs can be complex and prone to errors. In contrast, the blockchain-based system ensures that all evidence related transactions are recorded in a decentralized and immutable ledger, significantly enhancing data integrity and trust.

From an operational perspective, the integration of blockchain technology with evidence management, case tracking, and inter-departmental coordination improves efficiency and accountability. Each action performed on forensic evidence—such as submission, transfer, verification, and reporting is securely recorded as a transaction, allowing real time tracking and complete traceability. This eliminates manual record keeping errors and reduces the chances of evidence manipulation. Compared to traditional methods, the system minimizes administrative overhead, automates verification processes, and ensures accurate and transparent handling of forensic data.

In terms of user experience, the system provides a structured and role-based interface for Admin, Police, Hospital staff, Lab technicians, and Doctors. Users can easily access relevant information, update case statuses, and verify reports within a secure environment. Authentication and access control mechanisms ensure that only authorized personnel can interact with sensitive data. The transparency provided by blockchain enhances trust among stakeholders, including victims and legal authorities, by allowing them to track the status and handling of evidence.

Performance comparisons indicate that the blockchain based system improves the efficiency of forensic processes by reducing delays in evidence verification and report generation. It enhances coordination between departments and ensures faster decision making. The system also supports auditability, enabling administrators to monitor activities, identify discrepancies, and maintain accountability. This leads to better resource utilization and improved overall system performance. Furthermore, the system introduces ethical and legal advantages by ensuring the authenticity and immutability of forensic evidence. The ability to trace the complete history of evidence handling discourages malpractice and strengthens the judicial process. Unlike traditional systems, which may lack proper monitoring and transparency, this approach ensures compliance with legal standards and promotes trust in digital investigations.

Overall, the blockchain-based forensic evidence management system demonstrates superior security, efficiency, and transparency compared to traditional methods. By integrating decentralized technology with forensic workflows, it provides a reliable, tamper-proof,and scalable solution that enhances the credibility and effectiveness of forensic investigations in the digital era.

8. Conclusion & Future Scope

The proposed system for Security Enhancement of Forensic Evidences Using Blockchain has been successfully designed, implemented, and evaluated, demonstrating significant improvements in the integrity, transparency, and reliability of forensic evidence management. The system effectively utilizes Blockchain Technology to create a decentralized and tamper-proof environment where all evidence-related activities are securely recorded. The integration of Cryptographic Hashing ensures that each piece of evidence is uniquely identified and protected against unauthorized modifications, while Smart Contracts enable automated access control and verification processes, reducing human intervention and the possibility of errors.

The system demonstrated reliable performance in maintaining a secure chain of custody by continuously recording evidence collection, access, transfer, and analysis as immutable transactions on the blockchain. Real-time monitoring and data accessibility through a web-based interface allow investigators, forensic experts, and legal authorities to verify evidence authenticity and track its history efficiently. The decentralized architecture eliminates single points of failure and enhances resistance against cyber threats, ensuring high system availability and robustness.

Integration with cloud-based platforms further enables efficient data visualization, auditing, and remote accessibility, making the system practical and user-friendly. Continuous testing confirmed seamless interaction

between system components, validating its reliability and effectiveness in real-world forensic scenarios. Overall, the proposed system provides a secure, transparent, and efficient solution for forensic evidence management, significantly improving trust and admissibility in legal proceedings. Future enhancements may include the incorporation of advanced analytics, artificial intelligence for evidence pattern recognition, and interoperability with national or global forensic databases to further strengthen the system's capabilities.

The feature scope of a system designed for Security Enhancement of Forensic Evidences Using Blockchain can be understood in a more practical and user-friendly way as a secure and reliable platform that helps investigators handle digital evidence without fear of tampering or loss. The system begins by safely collecting evidence from devices like computers, mobile phones, or network systems, and assigns each piece a unique digital fingerprint using Cryptographic Hash Functions. This fingerprint ensures that even the smallest change in the evidence can be detected immediately.

Once collected, all actions performed on the evidence such as who accessed it, when it was transferred, or how it was analyzed are recorded on a blockchain, creating a transparent and permanent record. This acts like a digital logbook that cannot be altered, helping maintain trust throughout the investigation process. The system also uses Smart Contracts to automatically control who is allowed to access or modify the evidence, reducing human error and ensuring that only authorized personnel are involved. To keep the system efficient, the actual evidence files are stored securely outside the blockchain, while only important details and verification data are stored on it. Investigators and legal authorities can easily verify whether the evidence is original and unchanged at any time, which is especially important in court proceedings. Additionally, the system can integrate with existing forensic tools, send alerts if any suspicious activity is detected, and use encryption and digital signatures to further protect sensitive data.

References

[1] A. Sharma and R. K. Singh, "A Decentralized Framework for Digital Forensic Chain of Custody using Ethereum Smart Contracts," *IEEE Trans. Inf. Forensics Secur.*, vol. 21, pp. 412–425, Jan. 2026.
[2] X. Li, J. Wang, and M. Zhang, "Blockchain-Based Secure Storage and Sharing of Multimedia Forensic Evidence," *Comput. Secur.*, vol. 148, Art. no. 103652, Nov. 2025.
[3] S. Nair and P. V. Reddy, "Integrity Verification of IoT Forensic Data via Consortium Blockchain and IPFS," *J. Digit. Forensic Pract.*, vol. 17, no. 2, pp. 110–124, May 2025.
[4] "The Application of Blockchain Technology in the Field of Digital Forensics: A Systematic Literature Review," *MDPI Digit.*, vol. 3, no. 1, Feb. 2025.
[5] "Blockchain Based Framework for Securing Digital Evidence: Immutability and Traceability," in *Proc. Int. Conf. Cloud Comput. Cybersecur. (ICCCC)*, 2025.
[6] "An Analysis of Blockchain Solutions for Digital Evidence Chain of Custody: Alignment with ISO 27037," *ResearchGate Preprints*, May 2025.
[7] H. Al-Azzam and M. Al-Rousan, "A Blockchain-Based Solution for Protecting the Integrity of Digital Evidence in Cybercrime Investigations," *Sensors*, vol. 24, no. 8, p. 2451, Apr. 2024.
[8] V. Gupta and S. Tyagi, "Secure Forensic Data Management: A Hybrid Approach using AI and Blockchain," in *Proc. 18th Int. Conf. Netw. Syst. Secur. (NSS)*, pp. 301–315, 2024.
[9] A. A. Khan and M. Zakaria, "Blockchain for Digital Forensics: Challenges, Opportunities, and Open Problems," *Forensic Sci. Int. Digit. Investig.*, vol. 45, Art. no. 301542, 2023.
[10] J. Rodriguez, "Proof-of-Stake Consensus for Energy-Efficient Evidence Logging in Forensic Networks," *Int. J. Inf. Secur.*, vol. 22, no. 4, pp. 567–580, 2023.