IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 4, April 2025

Impact Factor: 7.67

Forensic Evidence Protection System Using Blockchain Technology

Dr. K. Chaitanya[1], K.Pravallika[2], G.Hari Narayana[3], SK. Shamshoon[4]

Associate Professor, Department of Computer Science and Engineering[1]

Students, Department of Computer Science and Engineering[2,3,4]

SRK Institute of Technology, Vijayawada, Andhra Pradesh, INDIA

Abstract: *In the digital era, maintaining the integrity and authenticity of forensic evidence is critical to ensuring justice and transparency. This 'Forensic Evidence Protection System Using Blockchain Technology' presents a secure and tamper-proof solution for storing and managing digital forensic evidence. The system allows a single authenticated user to register and log in to a web-based platform to upload forensic evidence files. Once uploaded, the file is processed and stored within a blockchain ledger to ensure immutability and transparency.*

Each uploaded file is encapsulated in a new block that contains key attributes, including an index, evidence hash, timestamp, previous hash, nonce, block hash, file name, and allowed actions. The blockchain ledger ensures that evidence cannot be altered once added, and any attempt to tamper with the data triggers a warning alert. Users can download the proof and verify its integrity using the evidence hash, thus confirming that the data remains unmodified. This system effectively utilizes blockchain's decentralized and secure nature to protect the chain of custody for digital forensic evidence.

Keywords: Blockchain, Digital Forensics, Cybersecurity, Evidence Integrity, SHA-256, AES Encryption, Tamper-Proof Storage

I. INTRODUCTION

In the modern digital era, the protection and management of forensic evidence are critical concerns in various sectors, including legal, financial, and educational institutions. The authenticity, integrity, and security of digital evidence play a pivotal role in ensuring fair judicial processes and maintaining the credibility of investigations. However, traditional forensic evidence management systems often face significant challenges, including vulnerability to tampering, unauthorized access, and inefficiencies in retaining a reliable chain of custody. The evolution of cyber threats, digital fraud, and data manipulation further exacerbates these issues, necessitating the development a more secure and robust approach to forensic evidence management.

Blockchain technology presents a transformative solution to address these challenges by offering a decentralized, tamper-resistant, and transparent framework for evidence management. Blockchain, a distributed ledger technology, ensures that data is recorded immutable, and verifiable, preventing unauthorized modifications and guaranteeing the authenticity of forensic evidence. By leveraging cryptographic techniques, blockchain enables secure data storage while maintaining the privacy of sensitive information, making it an ideal solution for forensic applications.

Furthermore, the contradiction between the traceability and privacy of forensic evidence is a significant concern in digital forensics. While blockchain provides a transparent and publicly verifiable ledger, certain evidence requires confidentiality to protect sensitive information. To address this, advanced cryptographic techniques such as zero-knowledge proofs, secure multi-party computation, and Attribute-Based Encryption (ABE) can be integrated within the blockchain framework. These privacy-preserving mechanisms ensure that only authorized personnel can access and verify specific pieces of evidence while maintaining an auditable record of transactions.

Additionally, forensic investigations often generate large volumes of digital evidence, leading to significant storage and scalability challenges. Traditional blockchain networks face limitations in handling extensive datasets due to high computational requirements and storage constraints. To overcome this, hybrid blockchain architectures that integrate

DOI: 10.48175/IJARSCT-25178

off-chain storage solutions, such as InterPlanetary File System (IPFS), can be utilized. By storing metadata and cryptographic hashes on-chain while keeping the actual evidence files off-chain, this approach optimizes performance without compromising security and integrity.

The implementation of a blockchain-based forensic evidence protection system has far-reaching implications for law enforcement agencies, judicial bodies, and forensic laboratories. By automating evidence tracking and verification, the system streamlines forensic workflows, reduces human errors, and enhances operational efficiency. Moreover, smart contracts—self-executing digital agreements—can be deployed to enforce predefined rules and automate evidence-handling procedures, further strengthening the credibility of forensic investigations.

The purpose is to develop and implement a blockchain-based forensic evidence protection system to address the challenges associated with evidence tampering, unauthorized access, and inefficiencies in traditional forensic management practices. By demonstrating the effectiveness of blockchain in securing forensic evidence, this system seeks to enhance trust, accountability, and transparency within the judicial system, ultimately contributing to the integrity of legal proceedings and ensuring justice is served

II. LITERATURE SURVEY

1. Blockchain in Digital Forensics

The integration of blockchain technology into digital forensics has been widely explored due to its ability to provide secure, tamper-proof records. Blockchain's **immutability** and **transparency** make it an ideal solution for managing forensic evidence.

Zohdy et al. (2019) explored the use of blockchain for **digital evidence management**, emphasizing its potential to secure the integrity of data used in criminal investigations. Their work highlights how blockchain can be used to manage digital forensic evidence by tracking the chain of custody and preventing evidence tampering, which is crucial in maintaining the credibility of digital evidence.

2. Blockchain for Chain of Custody

One of the key concerns in digital forensics is the **chain of custody**—the documentation and protection of evidence as it moves through the legal and investigative process. Blockchain has shown great promise in addressing this concern.

Greene et al. (2017) proposed using blockchain to maintain the **chain of custody** in digital forensic investigations. Their system uses blockchain to create an immutable log of custody events, including timestamps and digital signatures, for each piece of evidence. This approach ensures that the evidence cannot be tampered with during its handling and transfer through the investigative process.

3. Blockchain-based Evidence Storage Systems

Another area of research has focused on how blockchain can be used to securely store **digital forensic evidence**. Storing evidence in a decentralized, immutable ledger ensures that it is protected from tampering.

Wang et al. (2018) explored blockchain-based evidence storage system where digital evidence is hashed and then stored in the blockchain. The authors argued that blockchain's inherent characteristics—like immutability and distributed consensus—provide a high level of security for forensic evidence. The system allows investigators to confirm that evidence has not been altered from the time it was captured.

III. METHODOLOGY

This system was built using Python and the Flask web framework. It uses a custom blockchain algorithm implemented from scratch and supports encrypted evidence storage.

Steps Involved:

1. User Registration and Login: The system allows one user to create an account. This is to ensure that only authorized personnel handle the evidence.

2. Evidence Upload: After login, the user can upload digital files such as documents, images, or logs. These files are encrypted using AES and hashed using SHA-256.

3. Blockchain Block Creation: A new block is created for each file. The block contains metadata like timestamp, hash, filename, previous block hash, evidence hash and nonce.
4. Integrity Verification: Each block is linked to the previous one using its hash. Any changes in one block break the chain and trigger a tampering alert.
5. Download and Verification: Users can download the file and verify it by using the SHA-256 hash

IV. EXISTING SYSTEM

Current forensic evidence systems often use secure servers or cloud-based storage, protected by passwords and encryption. However, they face several problems:

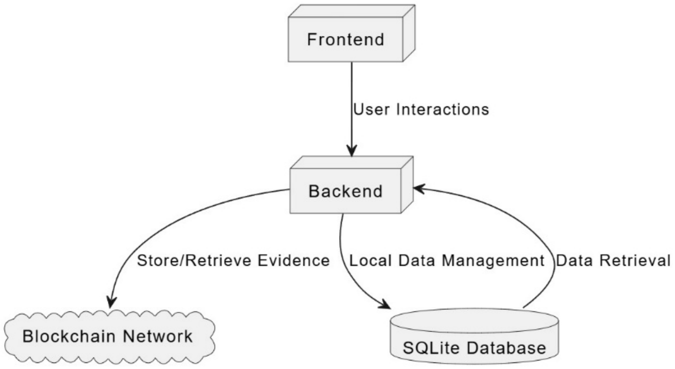
- **Centralized control** – A single point of failure
- **Tampering risk** – Data can be modified without detection
- **Lack of transparency** – No proof of when or by whom a file was changed

Disadvantages:

- Cannot track every action taken on evidence
- Difficult to prove that a file was never altered
- Vulnerable to data loss or unauthorized access
- These limitations reduce the reliability of forensic evidence in court or during investigations.

V. PROPOSED SYSTEM

The proposed system is a secure, blockchain-based platform that ensures digital forensic evidence cannot be tampered with. It provides a single user interface where one person can register and manage all evidence files.



1. Frontend (User Interface)

Purpose: Acts as the entry point for the user (only a single authorized person).

Functionality:

- Allows secure login.
- Enables the user to upload forensic evidence files (images, documents, etc.).
- Provides visual confirmation of successful uploads and verification results.

2. Backend (Application Logic)

Acts as the core processing engine that connects all parts of the system.

Handles all logic related to:

- **User interactions** from the front end.
- **File processing**, including hashing for blockchain storage.
- **Communication with the Blockchain Network** and **SQLite Database**.

3. SQLite Database (Local Data Storage)
Purpose: Stores non-sensitive metadata and supports local operations.
Functionality:

- Stores filenames, upload timestamps, and user activity logs.
- It supports **local data management** and **data retrieval** for quicker access and reporting.
- Does **not** store the actual files or hashes permanently (those are on the blockchain).

4. Blockchain Network (Immutable Storage)
Purpose: Provides tamper-proof storage and verification.
Functionality:

- Stores the cryptographic **hash of the uploaded file** as a block entry.
- During verification, a file's hash is recalculated and compared with the hash on the blockchain.
- Guarantees the **integrity and immutability** of forensic evidence.

5. Data Flow Summary (Based on Diagram)
The user logs in via the **front end** and uploads a file.
The **Backend** receives the file:

- Stores metadata locally in the **SQLite Database**.
- Computes a **hash of the file** and sends it to the **Blockchain Network** for storage.
- When the file is accessed later, the **Backend**:
- Retrieves metadata from **SQLite**.
- Recalculates the file hash and verifies it against the **Blockchain ledger**.
- The verification result is shown on the **front end**, confirming whether the evidence has remained untampered.

Proposed Blockchain-Based Forensic Evidence Protection System and Its Benefits
Decentralized and Tamper-Resistant Evidence Storage
The proposed system leverages blockchain technology to provide a decentralized and tamper-resistant storage mechanism for forensic evidence. Unlike traditional centralized databases, blockchain operates on a distributed ledger, ensuring that every piece of evidence recorded is immutable and cannot be altered or deleted by any single entity. Each evidence record is stored as a cryptographically secured transaction, making it impossible for unauthorized modifications to take place. This eliminates the risk of evidence tampering and enhances the overall security of forensic data, ensuring that investigations are based on authentic and verifiable evidence.

Enhanced Chain of Custody Management
Maintaining a transparent and verifiable chain of custody is one of the most critical aspects of forensic evidence management. The proposed system integrates smart contracts within the blockchain framework to automate the chain of custody tracking. Every action taken on a piece of evidence, including its collection, transfer, analysis, and presentation in court, is recorded on the blockchain in a time-stamped and cryptographically secured manner. This ensures that the integrity of evidence is maintained throughout its lifecycle, preventing unauthorized handling and providing a clear audit trail that can be independently verified by legal authorities.

Increased Transparency and Trust
Blockchain technology enhances transparency by allowing authorized stakeholders, including forensic investigators, legal professionals, and law enforcement agencies, to access and verify the authenticity of forensic evidence in real-time. The decentralized nature of the system ensures that no single entity has complete control over the evidence records, eliminating concerns related to biased alterations. By providing an immutable and publicly verifiable ledger,

DOI: 10.48175/IJARSCT-25178

the proposed system fosters trust among judicial bodies and ensures that forensic evidence is handled in a fair and accountable manner.

Secure and Scalable Digital Evidence Storage

The proposed system addresses the challenges of storing and managing large volumes of forensic evidence by integrating blockchain with decentralized storage solutions such as the InterPlanetary File System (IPFS). While blockchain records cryptographic hashes and metadata, actual evidence files are securely stored off-chain, ensuring scalability without compromising security. This hybrid storage approach enables efficient retrieval and management of large forensic datasets, including multimedia files, documents, and encrypted records. By distributing evidence storage across a decentralized network, the system mitigates the risks associated with centralized data breaches and unauthorized access.

Privacy-Preserving Mechanisms

Forensic evidence often contains sensitive information that requires strict privacy controls. The proposed system incorporates advanced cryptographic techniques such as Attribute-Based Encryption (ABE), zero-knowledge proofs, and secure multi-party computation to ensure privacy while maintaining transparency. These mechanisms allow only authorized personnel to decrypt and access specific evidence records without exposing confidential details to unauthorized individuals. By implementing fine-grained access control policies, the system ensures that sensitive forensic data is protected while remaining verifiable when required in legal proceedings.

Automated Smart Contract Execution

Smart contracts play a crucial role in automating various forensic evidence management processes, reducing human errors, and enhancing operational efficiency. In the proposed system, smart contracts enforce predefined rules related to evidence collection, verification, and presentation. For example, when a piece of evidence is collected, a smart contract can automatically trigger notifications to relevant stakeholders, record its timestamp on the blockchain, and assign digital signatures to ensure authenticity. By eliminating manual intervention, smart contracts enhance the accuracy, speed, and reliability of forensic workflows.

Strengthened Cybersecurity Measures

Cyber threats such as hacking, ransomware attacks, and unauthorized access attempts pose significant risks to forensic evidence stored in traditional systems. The proposed blockchain-based system enhances cybersecurity by employing robust encryption, multi-signature authentication, and distributed consensus mechanisms. Each transaction recorded on the blockchain undergoes a validation process through consensus protocols, ensuring that only legitimate changes are accepted. Additionally, the use of decentralized identity management reduces the risk of insider threats by preventing unauthorized personnel from accessing or altering forensic data.

Efficient Cross-Jurisdictional Collaboration

Forensic investigations often involve multiple law enforcement agencies, forensic laboratories, and legal entities operating across different jurisdictions. The proposed system facilitates seamless cross-jurisdictional collaboration by providing a unified and standardized digital forensic evidence management platform. Since blockchain operates as a decentralized ledger accessible to authorized entities worldwide, investigators from different regions can securely access and verify evidence records without delays or jurisdictional conflicts. This improves coordination among forensic teams and ensures that evidence integrity is maintained across borders.

Legal and Regulatory Compliance

The proposed system is designed to align with legal and regulatory requirements governing forensic evidence management. By integrating blockchain-based digital signatures, timestamps, and verifiable cryptographic proofs, the system ensures that forensic evidence meets admissibility standards in court. Additionally, smart contracts can be programmed to enforce compliance with regional and international forensic guidelines, automatically flagging any discrepancies or unauthorized modifications. This enhances the credibility of digital evidence and strengthens its legal standing in judicial proceedings.

Cost-effective and Sustainable Forensic Management

Traditional forensic evidence management systems require extensive resources for maintaining centralized databases, securing digital storage, and managing chain of custody documentation. The proposed blockchain-based system significantly reduces operational costs by eliminating intermediaries, automating processes, and leveraging decentralized infrastructure. By minimizing the reliance on paper-based documentation and manual verification procedures, the system streamlines forensic workflows, reduces administrative burdens, and optimizes resource utilization. Additionally, the decentralized nature of blockchain ensures long-term sustainability by preventing single points of failure and enhancing system resilience against cyber threats.

VI. CONCLUSION

To sum up, the suggested blockchain-based SHA-256 encryption Forensic evidence management system offers a strong and creative response to the problems associated with protecting digital identities. The system assures data integrity, user privacy, and secure forensic evidence in addition to establishing a decentralized and transparent framework via the integration of modules including Login, User Signup, Home, Keys, Data, and Authenticate. User-friendly input and output interfaces are given priority in the design, which improves usability and accessibility. The system's objective is to mitigate the dangers associated with centralized forensic evidence management and promote confidence in an increasingly digital environment by offering a dependable and robust platform for users and banks, via methodical testing and deployment. Because of the thorough methodology used throughout the development and implementation phases, the system is positioned as a viable and efficient means of handling the ever-evolving complexity of Forensic evidence management.

VII. FUTURE ENHANCEMENT

Further exploration into these future enhancements will yield insights into how they can synergistically interact to create more secure and efficient blockchain-based forensic evidence handling systems. The convergence of biometric authentication, smart contracts, decentralized storage, real-time alerts, and varied blockchain options has the potential to significantly enhance digital forensic investigations, effectively combatting growing cybercrime challenges. As technology continues to advance, the implications of these enhancements necessitate ongoing evaluation to ensure they align with best practices and legal standards within the forensic community. Adapting to new technological frameworks will be key to evolving digital forensic methodologies and fortifying them against future threats.

REFERENCES

[1]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*. In 2017 IEEE International Congress on Big Data. https://ieeexplore.ieee.org/document/8029379

[2]. Kshetri, N. (2018). *1 Blockchain's roles in strengthening cybersecurity and protecting privacy*. Telecommunications Policy, 42(4), 313–331. https://doi.org/10.1016/j.telpol.2017.12.003

[3]. Wazid, M., Das, A. K., Bera, B., & Rodrigues, J. J. P. C. (2019). *Blockchain-Based Secure Storage Management with Enhanced Privacy and Reliability in Cloud Environment*. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2019.01.021

DOI: 10.48175/IJARSCT-25178