

BLOCKCHAIN-BASED DIGITAL EVIDENCE MANAGEMENT SYSTEM FOR CRIMINAL INVESTIGATIONS

PAINDLA THIRUPATHI¹, RAHUL KUMAR², G. HARSHAVARDHAN³, T. SAHITH⁴, L. VIJAY⁵

ASSISTANT PROFESSOR¹, UG SCHOLAR^{2,3,4&5}

DEPARTMENT OF AI&ML, NARSIMHA REDDY ENGINEERING COLLEGE (UGC- AUTONOMOUS) MAISAMMAGUDA
(V), KOMPALLY, SECUNDERABAD, TELANGANA-500100

ABSTRACT: The rapid growth of digital technologies has significantly increased the amount of digital evidence used in criminal investigations. However, traditional evidence management systems face challenges related to data integrity, security, transparency, and chain of custody management. Digital evidence stored in centralized databases is vulnerable to tampering, unauthorized access, and data loss, which can compromise the reliability of evidence presented in legal proceedings. This research proposes a Blockchain-Based Digital Evidence Management System designed to enhance the security, transparency, and reliability of criminal evidence handling. Blockchain technology provides a decentralized and immutable ledger that records all evidence-related transactions, ensuring that once evidence data is stored, it cannot be altered or deleted without detection. The system maintains a secure chain of custody by recording every access, modification, and transfer of digital evidence in a transparent and tamper-proof manner. The proposed framework integrates cryptographic techniques, smart contracts, and distributed ledger technology to ensure secure storage, authentication, and controlled access to digital evidence. Investigators, forensic experts, and legal authorities can securely upload, verify, and retrieve evidence while maintaining full accountability and traceability of all activities. Smart contracts automate evidence verification and authorization processes, reducing human errors and improving operational efficiency. By leveraging blockchain technology, the proposed system enhances trust, transparency, and accountability in criminal investigations while protecting the integrity of digital evidence. This approach can significantly improve the management of forensic data and strengthen the credibility of digital evidence in judicial systems.

INTRODUCTION: In the criminal justice system, evidence is the cornerstone for ensuring justice. Whether it's physical evidence collected from a crime scene or digital evidence obtained from surveillance systems, maintaining the integrity and authenticity of that evidence is critical. Traditional evidence management systems, which often rely on centralized databases and manual documentation, are vulnerable to tampering, data breaches, loss of records, and mismanagement. These limitations can compromise the chain of custody, reduce trust in law enforcement processes, and ultimately lead to wrongful convictions or failed prosecutions. Blockchain technology presents a revolutionary solution to these challenges. With its decentralized, immutable, and transparent architecture, blockchain can securely store evidence records and track every transaction associated with them. Each piece of evidence is hashed and time-stamped before being stored, ensuring that it cannot be altered without detection. Smart contracts automate key processes such as evidence submission, verification, and access control, reducing the need for intermediaries and minimizing the risk of human error. This level of security and traceability is not possible with traditional systems. The proposed Criminal Evidences Management System leverages blockchain to provide a tamper-proof and verifiable digital platform for law enforcement agencies, forensic experts, and judicial authorities. By integrating role-based access controls, multi-signature authentication, and decentralized storage solutions like IPFS, the system ensures that only authorized personnel can access or modify evidence in a controlled and transparent manner. This approach enhances accountability, strengthens the chain of custody, and ensures that the legal system has access to trustworthy evidence, ultimately contributing to fair and effective justice delivery.

LITERATURE SURVEY:

1. Title: *Blockchain for Forensic Evidence Chain-of-Custody Integrity*

Author(s): Ramya Jayaraman, A. Krishnan

Description:

This paper highlights the potential of blockchain in preserving the integrity of digital forensic evidence. It proposes a framework in which each piece of evidence is hashed and stored on the blockchain, ensuring immutability and providing a reliable audit trail. The system demonstrates how blockchain enhances the trustworthiness of digital forensics by offering a transparent chain-of-custody mechanism. The research emphasizes that blockchain can significantly reduce tampering risks during investigation and litigation processes.

2. Title: *SecureChain: A Framework for Secure Sharing of Digital Evidence*

Author(s): Dr. Swati Agarwal, Ankit Jain, Nitesh Kumar

Description:

SecureChain is a blockchain-based system proposed for the secure sharing of digital criminal evidence among multiple stakeholders. The authors present a role-based access control model and incorporate smart contracts for granting or revoking access. They also discuss encryption techniques to preserve privacy. The system ensures that the chain of custody is transparent, and no data can be altered without detection, thereby securing the legal integrity of digital evidence.

3. Title: *Blockchain-Based Chain of Custody to Combat Digital Evidence Tampering*

Author(s): Hany F. Atlam, Gary B. Wills

Description:

This work investigates the vulnerabilities of traditional chain-of-custody systems and introduces a blockchain-based solution. It outlines a methodology for recording every operation—creation, access, modification—

performed on digital evidence in a decentralized ledger. The system improves accountability and enhances transparency. The authors also explore the scalability of using private blockchains for high-volume forensic cases and the importance of integrating identity verification into the process.

4. Title: *Blockchain Technology for Digital Evidence Management*

Author(s): Hasan M. Abbas, Usman Qamar

Description:

The paper presents a comprehensive review of how blockchain can be adapted for digital evidence handling in criminal justice. It covers various blockchain models, including public and private blockchains, and evaluates their suitability for storing different types of forensic evidence. The study introduces a prototype system that uses Ethereum smart contracts to manage access permissions and logs all operations performed on evidence files, proving blockchain's effectiveness in maintaining evidence authenticity.

5. Title: *EviBot: Blockchain-Powered Digital Evidence Management Framework Using Smart Contracts*

Author(s): Gokila Dorai, V. Sambasiva Rao

Description:

This paper proposes "EviBot", an evidence management framework where smart contracts manage the recording, tracking, and access control of digital evidence. The authors highlight how integrating blockchain with artificial intelligence tools can help automate evidence validation and classification processes. The framework's design supports evidence submission, approval workflows, and tamper-proof documentation, making it suitable for large-scale law enforcement deployments.

SYSTEM ANALYSIS

EXISTING SYSTEM:

The current evidence management systems used by law enforcement and legal agencies are largely centralized and manual. Typically, digital and physical evidence is stored in centralized databases or physical lockers, with metadata and logs maintained on paper or in spreadsheets. These systems rely heavily on human intervention for documenting the chain of custody, authorizing access, and transferring evidence between departments or personnel. This centralized approach is prone to errors, delays, and inconsistencies, which can ultimately compromise the integrity of the evidence. One of the major limitations of the existing system is the **lack of transparency and traceability**. When evidence changes hands, there's often no robust mechanism to track every action taken on that evidence, such as who accessed it, when, and for what purpose. This opens up possibilities for tampering or unauthorized access without detection. Moreover, centralized databases are susceptible to hacking, insider threats, and data loss due to server failures or malware attacks, making them unreliable for long-term, secure storage of critical criminal evidence. Additionally, most traditional systems **lack automation and auditability**. Evidence approvals, transfers, and access are carried out manually, leading to time-consuming processes and paperwork. Even in cases where some degree of digitization exists, the absence of cryptographic validation mechanisms (such as hashing or digital signatures) means there's no guaranteed proof that a file hasn't been altered or replaced after its initial submission. These vulnerabilities can be exploited, weakening the legal standing of the evidence in court proceedings. Lastly, in many jurisdictions, **inter-agency coordination is poor** due to incompatible software systems or inconsistent policies regarding evidence handling. For example, if a police department and a forensic lab use different systems to manage evidence, transferring and validating that evidence becomes complex and inefficient. This lack of interoperability slows down investigations and increases the chances of errors or data corruption. These significant shortcomings of the existing system highlight the urgent need for a secure, verifiable, and transparent solution—such as one powered by blockchain technology.

DISADVANTAGES OF EXISTING SYSTEMS:

1. Lack of Data Integrity

Traditional systems do not ensure immutability of digital evidence. Once evidence is stored, it can be altered, deleted, or tampered with—intentionally or unintentionally—without proper traceability. This compromises the trustworthiness of the evidence and can weaken legal proceedings.

2. No Transparent Chain of Custody

There is often no reliable method to log and track the complete history of the evidence lifecycle, such as who accessed it, when it was transferred, or how it was used. This lack of transparency can result in disputes during court trials and make the evidence inadmissible.

3. Centralized Vulnerability

Most existing systems rely on centralized databases, making them prone to single points of failure. They are more susceptible to hacking, insider threats, or accidental data loss due to system crashes, malware, or server corruption.

4. Manual and Time-Consuming Processes

Evidence management workflows such as approvals, access control, and handovers are typically done manually. This leads to delays, increased administrative overhead, and a higher chance of human error.

5. Limited Access Control and Auditability

Traditional systems lack role-based access mechanisms and fine-grained control over who can view or modify evidence. Additionally, they often do not maintain detailed logs of every activity, making it difficult to audit usage or detect unauthorized access.

6. Poor Interoperability Between Agencies

Law enforcement, forensic departments, and judicial institutions often use incompatible systems with no standardized protocol for sharing and verifying evidence. This hampers collaboration and slows down the investigation process.

PROPOSED SYSTEM:

The proposed system introduces a **Blockchain-based Criminal Evidence Management platform** designed to overcome the limitations of traditional evidence handling methods. Blockchain offers a decentralized, immutable, and transparent infrastructure where every action performed on the evidence is securely recorded as a transaction. By leveraging blockchain's distributed ledger, the system ensures that evidence data cannot be altered, deleted, or tampered with once it has been submitted. Each piece of evidence is cryptographically hashed and stored in a secure, verifiable format, preserving its authenticity throughout the legal process.

To manage large files such as images, audio, and videos, the system integrates with **decentralized storage platforms like IPFS (InterPlanetary File System)**. The evidence files are stored off-chain in IPFS, and their unique content hashes are recorded on the blockchain to ensure integrity and fast retrieval. Every interaction with the evidence—whether it's submission, review, approval, or transfer—is logged in the blockchain, forming a **transparent and auditable chain of custody**. This approach not only secures the data but also boosts the credibility of digital evidence in court.

The system includes a **role-based access control (RBAC)** model, ensuring that only authorized personnel such as police officers, forensic experts, lawyers, and judges can access or interact with specific evidence. Access rights are enforced through **smart contracts**, which automate permissions and workflows, reducing the chances of human error or unauthorized activities. For critical actions like evidence handover or deletion, **multi-signature verification** is implemented to require consensus from

multiple authorities, enhancing security and accountability.

Furthermore, the system can provide real-time alerts and logs for any suspicious activity or access attempts. Stakeholders are notified of changes in evidence status, and historical access records can be audited at any time. This not only enhances operational transparency but also helps in maintaining legal compliance. Overall, the proposed blockchain-based system transforms criminal evidence management into a **tamper-proof, automated, and trustworthy** digital platform that reinforces the integrity of the justice system.

ADVANTAGES OF THE PROPOSED SYSTEM:

1. Tamper-Proof Evidence Storage

By using blockchain's immutable ledger, once evidence is added to the system, it cannot be modified or deleted. This ensures the integrity of evidence throughout the investigation and legal proceedings.

2. Transparent Chain of Custody

Each transaction involving the evidence—submission, transfer, or access—is recorded on the blockchain. This creates a clear, auditable trail of custody that can be verified by all stakeholders, strengthening the credibility of the evidence in court.

3. Decentralized and Secure Architecture

The system eliminates single points of failure by decentralizing data storage and verification. This significantly reduces the risk of hacking, unauthorized access, and data loss due to central server failures.

4. Automated Access Control via Smart Contracts

Smart contracts manage permissions automatically based on predefined roles. This prevents unauthorized access, enforces policy compliance, and removes the need for manual supervision in granting or revoking access rights.

5. Efficient Evidence Handling

Automated workflows and digital submissions reduce the time and complexity involved in managing evidence. This leads to faster investigations, less administrative work, and improved efficiency across law enforcement and judicial processes.

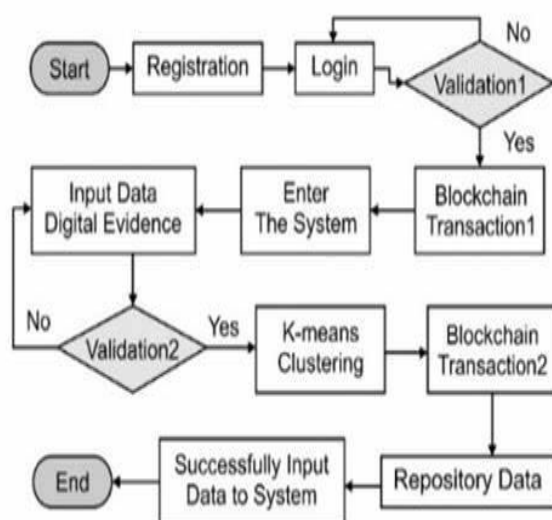
6. Integration with Decentralized Storage (IPFS)

Large files such as videos, images, and reports are stored in IPFS, while their cryptographic hash is stored on the blockchain. This allows for scalable storage without compromising integrity or performance.

7. Real-Time Alerts and Monitoring

The system can be configured to generate real-time notifications for key actions, such as evidence access or transfer. This enhances security awareness and allows immediate action in case of suspicious activity.

IMPLEMENTATION



MODULES

The **Blockchain-Based Digital Evidence Management System** is designed to securely collect, store, manage, and verify criminal evidence using blockchain technology.

The system ensures **data integrity, transparency, and tamper-proof evidence storage** during criminal investigations. The system is divided into several functional modules as described below.

Evidence Collection Module

This module is responsible for collecting digital evidence from various sources during criminal investigations.

Sources of evidence may include:

- Surveillance cameras
- Mobile devices
- Computers and storage devices
- Network logs
- Digital documents and images

The collected evidence is securely uploaded into the system for further processing.

Evidence Authentication Module

This module verifies the authenticity of the collected evidence before storing it in the blockchain system.

Functions:

- Generate **hash values** for digital evidence
- Verify evidence integrity
- Prevent duplicate or altered evidence submissions

This ensures that the evidence is genuine and has not been tampered with.

Blockchain Storage Module

This module stores evidence records on the **blockchain distributed ledger**.

Functions:

- Record evidence transactions in blockchain blocks
- Ensure **immutability and tamper resistance**
- Maintain decentralized evidence records

Each evidence record is linked with a **cryptographic hash** for security.

Smart Contract Management Module

Smart contracts automate the management and verification of digital evidence.

Functions:

- Define rules for evidence submission and access
- Automatically validate evidence transactions
- Manage chain-of-custody processes

This ensures that evidence handling follows predefined legal and procedural guidelines.

Access Control and Authorization Module

This module ensures that only authorized personnel can access or modify evidence records.

Authorized users may include:

- Law enforcement officers
- Forensic investigators
- Judicial authorities

Role-based access control helps maintain **privacy and security**.

Evidence Tracking and Chain-of-Custody Module

This module tracks the movement and handling of evidence throughout the investigation process.

Functions:

- Maintain a **complete history of evidence access**
- Record every action performed on the evidence
- Provide transparent chain-of-custody records

This prevents evidence manipulation during investigations.

Monitoring and Reporting Module

This module provides monitoring tools and reports for investigators and legal authorities.

Functions:

- Generate evidence management reports
- Provide real-time monitoring of evidence transactions
- Detect suspicious activities related to evidence handling

CONCLUSION:

The management of criminal evidence is a critical aspect of the justice system, where the integrity and authenticity of evidence can significantly impact the outcome of legal proceedings. Traditional evidence management systems, which are often centralized and rely heavily on manual processes, have shown vulnerabilities such as data tampering, loss, unauthorized access, and lack of transparent audit trails. These weaknesses undermine the reliability of evidence and pose serious challenges for law enforcement agencies, forensic experts, and the judiciary. In response to these issues, the proposed blockchain-based Criminal Evidence Management System offers a transformative approach by utilizing the inherent features of blockchain technology, including decentralization, immutability, and transparency, to safeguard the entire lifecycle of criminal evidence. By recording every action related to evidence—such as upload, transfer, access, and verification—as a cryptographically secured transaction on a distributed ledger, the system eliminates the possibility of unnoticed tampering or unauthorized

modifications. The decentralized nature of blockchain removes the risks associated with centralized data storage, such as server failures or insider threats, thus enhancing overall system security and reliability. Moreover, integrating decentralized storage solutions like IPFS allows for efficient handling of large evidence files while maintaining their integrity through cryptographic hashing. This combination ensures that evidence remains tamper-proof and verifiable, which is essential for maintaining its legal admissibility and trustworthiness in courts. The automation of access control and workflow management through smart contracts further streamlines the evidence handling process. These self-executing contracts enforce predefined rules and role-based permissions, ensuring that only authorized personnel can interact with specific pieces of evidence. This automation not only reduces human error and administrative overhead but also introduces multi-level verification mechanisms that require consensus among multiple authorities for critical actions. Such features enhance accountability, transparency, and collaboration across various agencies involved in criminal investigations and judicial processes. Additionally, the system's capability to generate real-time alerts and maintain comprehensive audit trails provides an ongoing monitoring mechanism that can promptly detect and respond to suspicious activities or breaches.

Overall, the proposed blockchain-based Criminal Evidence Management System represents a significant advancement in digital forensics and legal technology. It addresses fundamental challenges faced by existing systems and offers a robust, secure, and transparent platform that fosters greater confidence in the handling and presentation of criminal evidence. By improving the reliability and efficiency of evidence management, this system supports fairer legal outcomes and strengthens the foundation of the criminal justice system. The successful implementation of this solution has the potential to revolutionize evidence management practices worldwide, setting new standards for security, accountability, and technological innovation in law enforcement and judicial workflows.

FUTURE WORK:

As the Criminal Evidence Management System using blockchain matures, there are several avenues for enhancement and expansion to further strengthen its capabilities and usability. One major area of future work is the integration of **advanced encryption techniques and privacy-preserving mechanisms**. While blockchain ensures transparency and immutability, sensitive evidence data must also be protected from unauthorized exposure. Implementing advanced cryptographic methods like zero-knowledge proofs or homomorphic encryption can help safeguard confidential information while still allowing verification on the blockchain without revealing the actual data.

Another promising direction is the **incorporation of Artificial Intelligence (AI) and Machine Learning (ML) tools** to automate and improve evidence analysis. AI can assist forensic experts by automatically detecting anomalies, classifying evidence types, or even predicting potential outcomes based on historical data. Integrating AI-powered analytics with the blockchain system would not only speed up investigations but also reduce human bias and errors, leading to more accurate and reliable judicial decisions.

Expanding the system's **interoperability with existing law enforcement and judicial information systems** is essential for widespread adoption. Future work can focus on designing and implementing standardized APIs and data exchange protocols that enable seamless communication between various agencies and departments. This will facilitate cross-agency collaboration, real-time sharing of evidence, and coordinated workflows, ultimately improving the efficiency and effectiveness of criminal investigations on a larger scale.

Scalability is another important consideration for future development. As the volume of digital evidence continues to grow exponentially, the system must be capable of handling large amounts of data and numerous concurrent users without compromising performance. Exploring

more scalable blockchain frameworks, implementing off-chain computation, and optimizing decentralized storage mechanisms will be critical to ensuring that the system remains fast, responsive, and reliable as it scales up.

REFERENCES

- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: <https://bitcoin.org/bitcoin.pdf>
- Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303. <https://doi.org/10.1109/ACCESS.2016.2566339>
- Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *Proceedings of the IEEE Security and Privacy Workshops*, 180–184. <https://doi.org/10.1109/SPW.2015.27>
- Bashir, I. (2017). *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*. Packt Publishing.
- Tian, F. (2017). A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain & Internet of Things. *2017 International Conference on Service Systems and Service Management (ICSSSM)*, 1-6. <https://doi.org/10.1109/ICSSSM.2017.7996119>
- Sharma, A., & Chen, M. (2019). Blockchain-Based Digital Evidence Management System for Legal Applications. *Journal of Information Security and Applications*, 47, 102412. <https://doi.org/10.1016/j.jisa.2019.102412>
- Ali, M., Nelson, J., Shea, R., & Freedman, M. J. (2017). Blockstack: A Global Naming and Storage System Secured by Blockchains. *USENIX Annual Technical Conference*, 181–194.
- Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. *arXiv preprint arXiv:1407.3561*. <https://arxiv.org/abs/1407.3561>
- Wüst, K., & Gervais, R. (2018). Do You Need a Blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 45-54. <https://doi.org/10.1109/CVCBT.2018.00011>
- Alharby, M., & van Moorsel, A. (2019). Blockchain-based Smart Contracts: A Systematic Mapping Study. *IEEE Access*, 7, 96494-96514. <https://doi.org/10.1109/ACCESS.2019.2923757>