Security Enhancement of Forensic Evidences Using Blockchain

Jagdale Snehal[1], Nimse Rutuja[2], Pokharkar Kajal[3], Prof. Sinalkar M. G.[4]
[1,2,3,4] Computer Engineering, JCOE Kuran

Abstract- The traditional methods of handling forensic evidence are susceptible to manipulation and tampering, raising concerns about their integrity and admissibility in court. This project explores the potential of blockchain technology to enhance the security of forensic evidence. Blockchain, a decentralized and tamper-proof ledger system, offers several key advantages for forensic evidence management:

- **Immutability: Once data is recorded on the blockchain, it becomes virtually impossible to alter or delete, ensuring the authenticity and integrity of the evidence.**
- **Transparency: Every transaction involving the evidence, from collection to analysis, is securely recorded on the blockchain, promoting transparency and accountability throughout the chain of custody.**
- **Traceability: The complete history of the evidence can be easily traced on the blockchain, allowing for verification of its origin and handling at every stage.**

This project proposes a system that utilizes blockchain technology to manage and secure forensic evidence. The system offers a secure and transparent platform for handling evidence, potentially improving the reliability and effectiveness of the legal process.

Keywords: Blockchain, forensic evidence, security, integrity, transparency, chain of custody

1. INTRODUCTION

The integrity of forensic evidence is paramount in the legal system, as it forms the foundation for investigations, prosecutions, and ultimately, the pursuit of justice. However, traditional methods of evidence handling are vulnerable to various challenges:

- Manipulation: Evidence can be tampered with at various points in the chain of custody, raising concerns about its authenticity and raising doubts about the legitimacy of the case.
- Human Error: Accidental mishandling or loss of evidence can compromise its integrity and hinder investigations.
- Lack of Transparency: The traditional chain of custody system can be opaque, making it difficult to track the movement of evidence and raising concerns about accountability.

These issues highlight the need for innovative solutions to ensure the security and integrity of forensic evidence. This project introduces the potential of blockchain technology as a transformative tool for addressing these challenges and enhancing the reliability of the legal process.

The following sections will explore:

- An overview of blockchain technology and its key characteristics.
- How blockchain can address the vulnerabilities of traditional forensic evidence management. The potential benefits of implementing a blockchain-based system for handling forensic evidence.

2. LITERATURE REVIEW

1. Paper Name: Security Enhancement of Forensic Evidences Using Blockchain Author:Sonali Patil and Sarika kadam

In today's digital era, data is most important in every phase of work. The storage and processing on data with security is the need of each and every application field. Data need to be tamper resistant due to possibility of alteration. Data can be represented and stored in heterogeneous format. There are chances of attack on information which is vital for particular organization. With rapid increase in cyber crime, attackers behave maliciously to alter those data. But it is having great impact on forensic evidences which is required for provenance. Therefore, it is required to maintain the reliability and provenance of digital evidences as it travels through various stages during forensic investigation. In this approach, there i s a

forensic chain in which generated report passes through various levels or intermediaries such as pathology laboratory, doctor, police department etc. To build the transparent system with immutability of forensic evidences, blockchain technology is more suitable. Blockchain technology provides the transfer of assets or evidence reports in transparent environment without central authority. In this paper blockchain based secure system for forensic evidences is proposed.

2. Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology
Author name: MEHRAN POURVAHAB
Cloud forensics is an intelligent evolution of digital forensics that defends against cyber-crimes. However, centralized evidence collection and preservation minimizes the reliability of digital evidence. To resolve this severe problem, this paper proposes a novel digital forensic architecture using fast-growing Software-Defined Networking (SDN) and Blockchain technology for Infrastructureas-a-Service (IaaS) cloud. In this proposed forensic architecture, the evidence is collected and preserved in the blockchain that is distributed among multiple peers. To protect the system from unauthorized users, Secure Ring Verification based Authentication (SRVA) scheme is proposed. To strengthen the cloud environment, secret keys are generated optimally by using Harmony Search Optimization (HSO) algorithm. All data are encrypted based on the sensitivity level and stored in the cloud server. For encryption, Sensitivity Aware Deep Elliptic Curve Cryptography (SADECC) algorithm is presented. For every data stored in the cloud, a block is created in the SDN controller and the history of data is recorded as metadata. In each block, the Merkle ha sh tree is built by using Secure Hashing Algorithm-3 (SHA-3). Our system allows users to trace their data by deploying Fuzzy based Smart Contracts (FCS). Finally, evidence analysis is enabled by constructing Logical Graph of Evidence (LGoE) collected from the blockchain

3. Paper Name: An Implementation of Blockchain Technology in Forensic Evidence Management
Author:- Revathy Sathyaprakasan, Pratheeksha Govindan
Evidence management is crucial in the field of forensic science. Evidences obtained from a crime scene are important in solving the case and delivering justice to the parties involved. Hence, protecting these evidences from any form of alteration is of utmost important. Chain of Custody is the process which maintains the integrity of evidence. Inability to maintain the chain of custody will make the evidence inadmissible in court, eventually leading to the case dismissal. Digitalization of forensic evidence management system is a need of time as it is an environment friendly model. Blockchains are digitally distributed ledgers of transactions signed cryptographically in chronological order that are sorted into blocks and is completely open to anyone in the blockchain network. Hyperledger Fabric is a consortium blockchain framework created by the Linux foundation and is mainly used for enterprise use. Based on the concept of Hyperledger Fabric, present study aimed to create a framework and further propose an algorithm to implement Blockchain Technology to digitalize forensic evidence management system and maintain Chain of Custody

3.METHODOLOGY:

This project aims to develop a secure and transparent system for managing forensic evidence using blockchain technology. The methodology will involve the following stages:

1.Requirement Analysis:

- Identify specific needs and challenges: This involves consulting with legal professionals, forensic investigators, and other stakeholders to understand the current challenges and desired functionalities of a blockchain-based evidence management system.
- Define system requirements: Based on the analysis, a set of specific requirements will be formulated, outlining the functionalities, security considerations, and integration needs of the proposed system.

2.System Design and Architecture:

- Select suitable blockchain platform: This involves evaluating various existing blockchain platforms and choosing one that aligns with the identified requirements in terms of scalability, security, and compatibility with the legal system.
- Design the system architecture: This stage focuses

on defining the system's components, their functionalities, and interactions. This includes designing how evidence data will be structured, stored, and accessed on the blockchain, and how smart contracts will be used to automate specific workflows.

- Develop security protocols: Robust security measures will be designed to ensure the confidentiality, integrity, and availability of the evidence stored on the blockchain.

3. System Development and Implementation:

- Develop the system prototype: A functional prototype of the proposed system will be developed, demonstrating its core functionalities and user interface.
- Explore possibilities for integration with existing legal and forensic software systems to ensure seamless adoption and data exchange.
- Conduct testing and validation: The developed prototype will undergo rigorous testing to ensure functionality, security, and compliance with relevant regulations and standards.

4. Evaluation and Refinement:

- Evaluate the system performance: The performance of the prototype will be evaluated based on predefined metrics, such as transaction speed, scalability, and ease of use.
- Gather feedback from stakeholders: Feedback will be collected from various stakeholders, including legal professionals, forensic investigators, and potential users, to identify areas for improvement and refinement.
- Refine the system: Based on the evaluation and feedback, the system will be iteratively improved to address identified shortcomings and enhance its overall effectiveness

5. Proposed System:

This project proposes a novel system for managing forensic evidence, leveraging the advantages of blockchain technology to enhance security, transparency, and accountability.

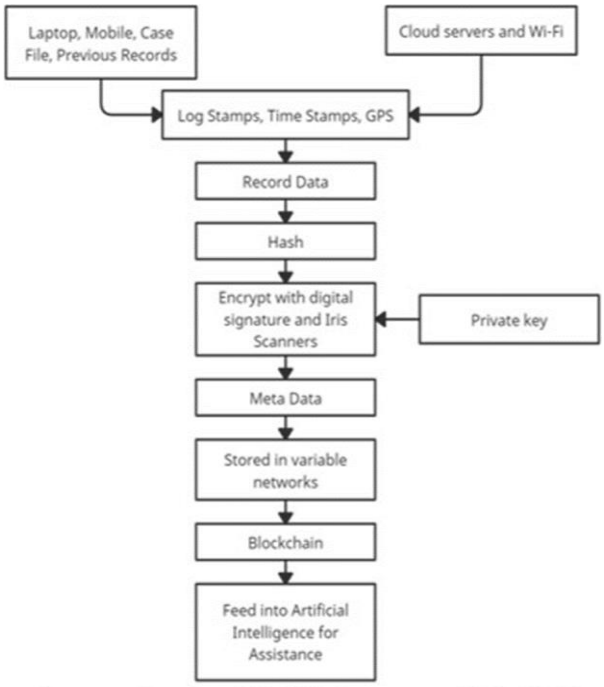


Figure 2.1-Flowchart of the link between AI-Blockchain [1]

1. System Architecture:

- Components:
  - Blockchain Network: A permissioned blockchain network will be established, allowing only authorized participants (e.g., law enforcement agencies, forensic labs, courts) to access and modify the evidence data.
  - Smart Contracts: These self-executing contracts will automate specific tasks within the evidence management process, such as:
    - Initiating chain of custody records upon evidence collection.
    - Triggering notifications for authorized personnel when evidence changes location or undergoes analysis.
    - Enforcing access control rules to ensure only authorized individuals can access specific evidence data.
  - Evidence Database: A secure, off-chain database will store the actual evidentiary data (e.g., digital files, images, videos) in a hashed format, ensuring data integrity while protecting sensitive information.
  - User Interface: A user-friendly interface will allow authorized personnel to interact with the system, view evidence information, and manage the chain of custody.

2. Workflow:

1. Evidence Collection: Upon collection, a unique identifier is assigned to the evidence, and its initial state, location, and custodian are recorded on the blockchain.
2. Chain of Custody Management: Every transfer of evidence between authorized entities is automatically recorded on the blockchain, creating an immutable and transparent history of its movement.
3. Evidence Analysis: Authorized forensic labs can access and analyze the evidence stored in the secure off-chain database. The results of the analysis are recorded on the blockchain, including timestamps and analyst information.
4. Evidence Sharing: Authorized parties can securely share evidence with each other through the platform, ensuring all participants have access to the latest information.
5. Dispute Resolution: The immutable record of the evidence on the blockchain can be used to verify its authenticity and resolve any disputes about its handling during legal proceedings.

3. Benefits:

1. Enhanced Security: Blockchain technology provides tamper-proof storage for evidence data, significantly reducing the risk of manipulation or tampering.
2. Improved Transparency: The complete chain of custody is recorded on the blockchain, increasing transparency and accountability throughout the evidence handling process.
3. Streamlined Workflow: Smart contracts automate tasks, reducing manual effort and streamlining the evidence management process.
4. Enhanced Collaboration: The system facilitates secure sharing of evidence among authorized personnel, fostering better collaboration between different stakeholders.
5. Increased Trust: The immutability and transparency of the system build trust in the handling of evidence, strengthening the legal process.

4. System Integration and Communication:

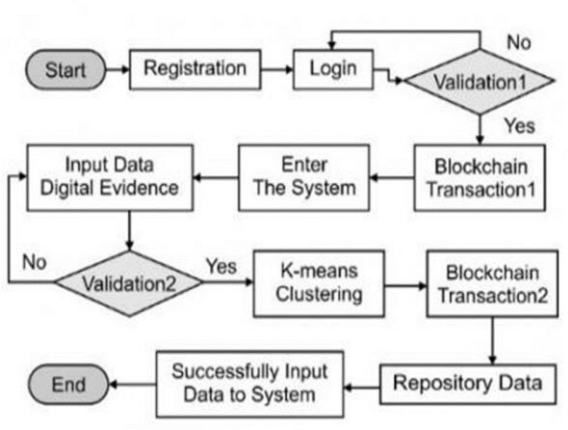
Seamless integratioThe proposed blockchain-based forensic evidence management system will need to integrate with various existing systems:

Law Enforcement Case Management Systems (LECMS): Seamless integration with existing LECMS will allow officers to initiate evidence entries, track chain of custody, and access relevant information directly within their familiar system.

5. Security and Redundancy:

The proposed system prioritizes security throughout its design and implementation to ensure the integrity and confidentiality of sensitive forensic evidence. Here are key security considerations:

6. Flow Chart:



7. Expected Result:

The Experiment Was Done On Forensic Evidences Using Blockchain.

8. Conclusion:

It provides a secure and transparent way to transfer digital assets without the need for intermediaries. While there are several challenges to overcome, such as scalability and security, blockchain technology has the potential to revolutionize the way we transfer and store value.

REFERENCE

[1] Sonali Patil,"Security Enhancement of Forensic Evidences Using Blockchain" , [Year 2021]. DOI: 10.1109/ICICV50876.2021.9388486.

[2] MEHRAN POURVAHAB,"Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology"[year 2019]. DOI:

10.1109/ACCESS.2019.2946978.

[3] Dr. Ch. Rupa,"Preserve Security to Medical Evidences using Blockchain Technology",[Year 2020]. DOI: 10.1109/ICICCS48265.2020.9120948.

[4] Revathy Sathyaprakasan,"An Implementation of Blockchain Technology in Forensic Evidence Management"[Year 2021]. DOI: 10.1109/ICCIKE51210.2021.9410791.

[5] Sotirios Brotsis,"Blockchain Solutions for Forensic Evidence Preservation in IoT Environments", [Year 2019]. DOI: 10.1109/NETSOFT.2019.8806675.