

Crime Evidence Management

Mohammed Arshad Hussain, G Akitha, Dudala Bhavya Sree

¹Assistant Professor, Department Of Cse, Bhoj Reddy Engineering College For Women, India.

^{2,3}B. Tech Students, Department Of Cse, Bhoj Reddy Engineering College For Women, India.

ABSTRACT

The secure management of digital crime evidence is a cornerstone of modern forensic science and legal proceedings. Current systems are plagued by vulnerabilities, data loss, and tampering due to their centralized architecture and manual handling. This paper presents a robust decentralized framework for Crime Evidence Management using Blockchain and InterPlanetary File System (IPFS). By leveraging Ethereum smart contracts for immutable logging and IPFS for secure file storage, the proposed system ensures evidence integrity, transparency, and traceability throughout its lifecycle.

The solution supports multiple stakeholders, including forensic lab incharges, doctors, sub-inspectors, and court clerks, by providing role-based access, tamper-proof records, and real-time updates. Developed using Flask (Python), Solidity, Ganache, and MetaMask, the application enables secure registration, evidence upload, validation, and court submission, with no risk of unauthorized data modification. Extensive testing demonstrated the system's reliability and scalability across forensic workflows. This work contributes to digital forensics by introducing a scalable, secure, and legally compliant platform for managing digital evidence.

Keywords: Blockchain, Crime Evidence, Digital Forensics, IPFS, Ethereum, Smart Contracts, Flask, Chain of Custody, MetaMask

The blockchain-based solution for crime evidence management is designed to address the critical need for secure, tamper-proof handling of digital evidence in the investigation process. By leveraging blockchain technology, this system offers a decentralized approach to storing and managing crime data, ensuring that all evidence is securely stored in an immutable ledger. This means that once evidence is entered into the system, it cannot be altered or tampered with, providing an added layer of security and trust throughout the investigative process. Whether dealing with sensitive digital crime data, audio or video recordings, or forensic reports, the blockchain solution ensures that each piece of evidence is protected against unauthorized access or modification. A key feature of this system is its immutable record capability. Every action taken on the evidence from collection to analysis to submission in court is recorded in the blockchain, creating a transparent and verifiable audit trail. This ensures the integrity of the Chain of Evidence, a critical component of legal proceedings, as it guarantees that evidence has not been tampered with during storage or transfer. The decentralized nature of blockchain also eliminates the risk of a single point of failure, reducing the likelihood of data breaches or corruption of records. The system includes transparent access controls, where only authorized personnel such as investigators, forensic analysts, or legal teams can access specific evidence, ensuring that confidentiality and integrity are maintained at all times. Access permissions can be tracked and logged in real-time, enabling the system

1. INTRODUCTION

to track who accessed the data, when, and for what purpose. This feature provides additional layers of accountability and helps safeguard the privacy and security of sensitive information. This innovative solution not only streamlines evidence management but also simplifies the investigation process, allowing investigators to have full confidence in the data they are working with. Whether it's handling digital footprints from cybercrimes or physical evidence in criminal investigations, this system ensures that evidence remains authentic and accessible throughout the entire investigative and judicial process. By combining blockchain's strengths in security, transparency, and efficiency, the solution upholds the principles of justice and ensures that investigations are conducted with the highest level of reliability and trustworthiness.

Existing System

In the Chain of Evidence (CoE) process, crime evidence is generated and handled by various intermediaries, such as the Police Department, Hospitals, Forensic Laboratories, and other departments involved in the investigation. The CoE documents every interaction with the evidence, from collection to storage and analysis, to maintain its integrity. This documentation is crucial for ensuring that the evidence remains trustworthy and admissible in court. Without proper documentation and handling, evidence can be deemed unreliable, undermining the case and potentially leading to the dismissal of charges. The primary goal is to preserve the authenticity of the evidence so that it can serve as proof of the crime and withstand scrutiny during the judicial process. To achieve this, it is essential that tampering and manipulation of the evidence be avoided at all costs. Each department or entity that handles the evidence must be carefully monitored to ensure that the chain of custody remains unbroken. Verification and validation of every entity that

interacts with the evidence are key steps in this process. This includes recording who accessed the evidence, when it was handled, and what actions were taken, ensuring that no unauthorized changes or tampering occurred. These procedures provide an audit trail that ensures the evidence is handled appropriately at every stage, and ultimately, ensures that the evidence remains valid and admissible in court, maintaining its role in supporting the truth and upholding justice.

Proposed System

The proposed system uses a decentralized network of nodes to securely store digital evidence, eliminating the risks associated with a single point of failure. By distributing the data across multiple nodes, the system ensures redundancy, which means that even if one node fails or is compromised, the evidence remains accessible and intact. Each transaction, from evidence collection to analysis, is cryptographically recorded on the blockchain, which creates an immutable and transparent chain of custody. This ensures that evidence cannot be altered or tampered with at any point in the process, providing a reliable and verifiable history that can be used in court to support the authenticity of the evidence.

2. LITERATURE SURVEY

Jamulkar et al. (2021) proposed a blockchain-based system for evidence handling, emphasizing the importance of immutability and transparency in criminal investigations. Their use of blockchain to store evidence hashes aligns with our project's objective of ensuring tamper-proof digital records through Ethereum smart contracts.

Ashitha et al. (2023) introduced a decentralized forensic framework that used blockchain to verify evidence authenticity. However, their system lacked a scalable storage solution for multimedia evidence.

Our project addresses this limitation by integrating IPFS to securely store large digital files like images and reports.

Karthik et al. (2023) implemented ENIGMA, a secure forensic data sharing platform using blockchain. While their model focused on secure data transmission, it did not incorporate role-based access or automated workflows. In contrast, our system uses smart contracts to enforce role-specific functions for Lab In charge, Doctor, Sub Inspector, and Bench Clerk, improving accountability and auditability.

Moin et al. (2020) explored the use of smart contracts for legal document management but did not extend their work to forensic workflows. Our project builds on this concept by designing automated smart contract logic for evidence upload, validation, and court processing—enhancing both transparency and legal admissibility.

The National Institute of Standards and Technology (NIST) highlights the need for secure, traceable, and tamper-resistant systems in digital forensics. Our system meets these requirements through blockchain's immutable ledger and IPFS's decentralized storage, creating a transparent and verifiable chain of custody.

Studies on decentralized file systems like IPFS show increased data availability and resilience against single-point failures. These findings support our decision to use IPFS for storing large evidence files while storing only their cryptographic hashes on blockchain to ensure data integrity and efficient access.

Recent research also emphasizes the importance of usability and accessibility in forensic software. Our system is built using Flask and MetaMask, providing a lightweight and user-friendly interface for investigators, doctors, and legal professionals.

Existing studies validate the use of blockchain and IPFS in forensic and legal systems. However, most lack a complete integration of storage, smart contracts, and role-based workflows. Our project fills this gap by offering an end-to-end, tamper-proof, decentralized evidence management system tailored for real-world legal environments.

3. METHODOLOGY

Crime Evidence Management is developed using a layered modular architecture that ensures tamper-proof security, scalability, and role-based accessibility across stakeholders. The methodology involves the following structured components:

Software Architecture

Crime Evidence Management follows a four-tier architecture:

- **Frontend (Presentation Layer):** Designed using HTML, CSS, and Bootstrap for building clean, responsive user interfaces. Role-specific screens are provided for Forensic Lab In charge, Doctor, Sub Inspector, and Bench Clerk to ensure secure and guided access.
- **Backend (Application Logic Layer):** Implemented using Flask (Python), this layer handles all business logic, user requests, and interactions with smart contracts. The backend also controls role validation and evidence submission workflows.
- **Blockchain Layer:** Deployed using the Ethereum test network (Ganache), this layer records all critical transactions—such as evidence uploads, validations, and reports—on a secure, immutable blockchain ledger using Solidity smart contracts.
- **Storage Layer (IPFS Integration):** Evidence files are stored on the InterPlanetary File System (IPFS), a decentralized peer-to-peer storage network. Only the cryptographic hash of each file is recorded on the blockchain, ensuring data security, integrity, and verifiability.

- **MetaMask Authentication:** Used for secure login and user role identification. All blockchain interactions are authorized via MetaMask wallet signatures, ensuring that only verified users access the system.
- Workflow**
1. **User Registration and Authentication:** Users (Forensic Lab Incharge, Doctor, Sub Inspector, Bench Clerk) register through the frontend and authenticate using MetaMask. Role-based access is enforced via smart contracts.
 2. **Evidence Upload:** The Lab Incharge uploads digital evidence (e.g., images, PDFs) via the Flask-based web interface. Files are converted into cryptographic hashes and pinned to IPFS for decentralized storage.
 3. **Blockchain Logging:** After successful upload, the system logs the IPFS hash, evidence details, user role, and timestamp on the Ethereum blockchain via smart contracts, creating a tamper-proof audit trail.
 4. **Role-Based Validation:**
 - The **Doctor** logs in and validates the evidence, providing approval or comments.
 - The **Sub Inspector** reviews the validated evidence and submits a formal investigation report.
 - The **Bench Clerk** performs a final review of the complete case file and locks the evidence status for judicial submission.
 5. **Smart Contract Execution:** Each action—from upload to final verification—is processed through smart contract functions written in Solidity, ensuring secure and automated role-based logic.
 6. **Data Integrity and Traceability:** At every stage, the IPFS hash ensures that the evidence file remains untampered. All logs on the blockchain provide an immutable history for legal admissibility.
 7. **Planned Enhancements:** Future upgrades include integration with biometric authentication (e.g., Aadhaar), mobile application development for field officers, and automated alert systems for tamper detection.

4.RESULTS

The image showcases the web interface of “Crime Evidence Management”.

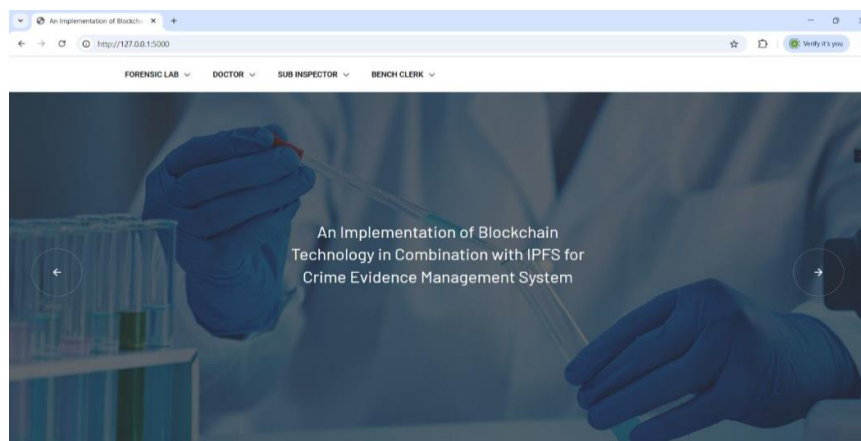


Fig 1 Home Page

After clicking on the Forensic Lab ,Below Forensic Lab In charge Registration Page appeared

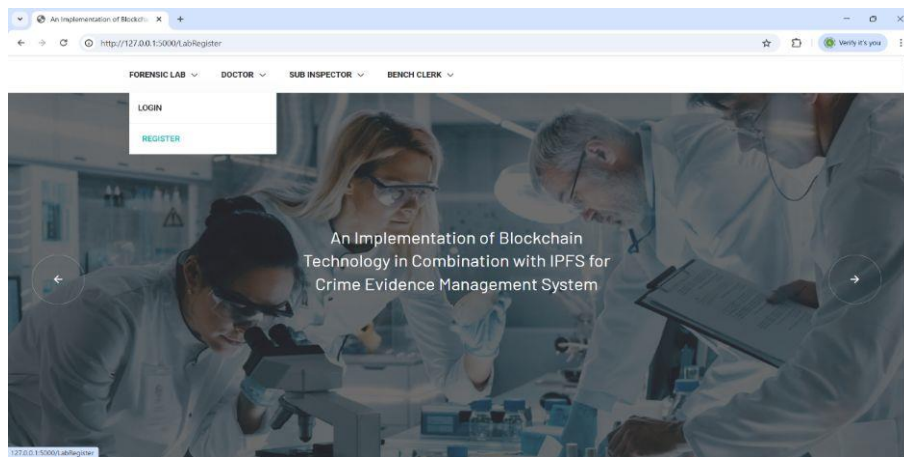


Fig:2 Forensic Lab In charge Registration

After successful Registration ,Forensic Lab In charge Login and Add's the Evidence

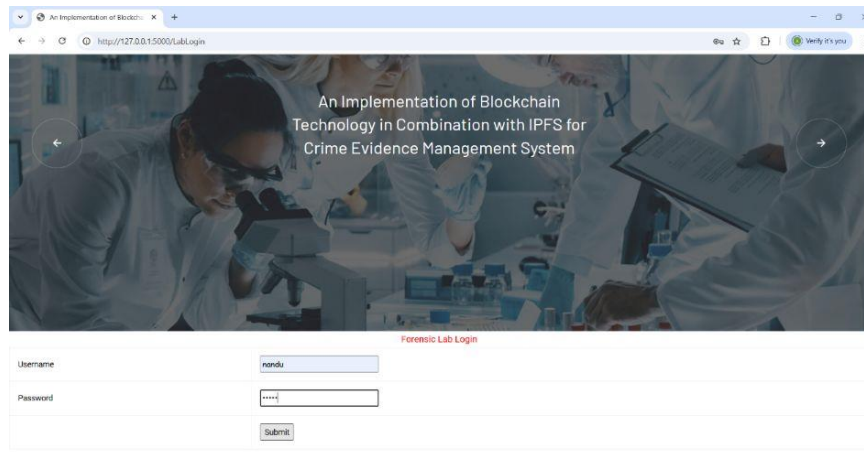


Fig 3 Forensic Lab In charge Login

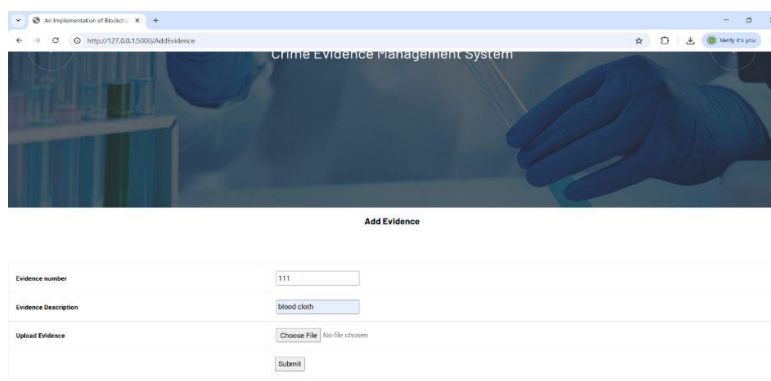
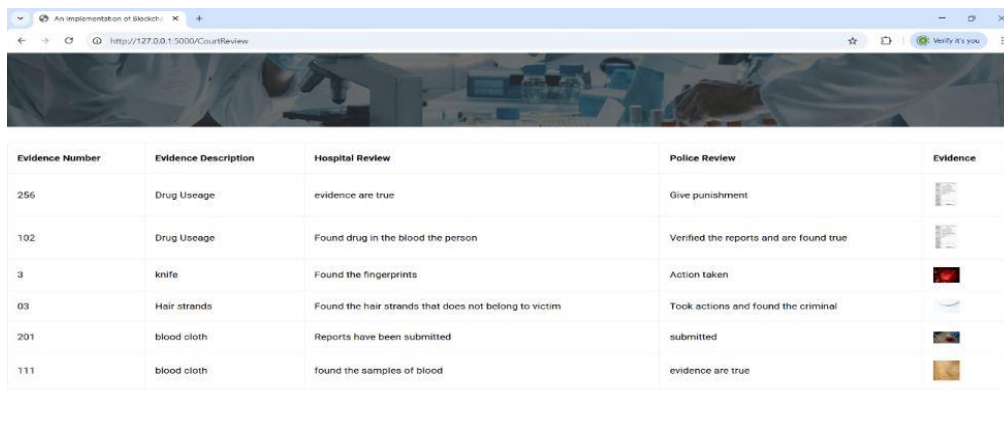


Fig 4: Add Evidence

Similarly Doctor Register and Login the Application and Check the Report and Add Review.

Sub Inspector checks the Police Review and the report , adds the details .

Bench Clerk Register and Login the Application and checks the Report.









Evidence Number	Evidence Description	Hospital Review	Police Review	Evidence
256	Drug Usage	evidence are true	Give punishment	
102	Drug Usage	Found drug in the blood the person	Verified the reports and are found true	
3	knife	Found the fingerprints	Action taken	
03	Hair strands	Found the hair strands that does not belong to victim	Took actions and found the criminal	
201	blood cloth	Reports have been submitted	submitted	
111	blood cloth	found the samples of blood	evidence are true	

Fig 5 Bench Clerk Checks the Report

5.CONCLUSION

The crime evidence management is securely digitized through blockchain and IPFS, ensuring integrity and transparency within the Chain of Evidence. This scalable system eliminates intermediaries, provides tamper-proof records, and enhances collaborative investigations and trust in the digital evidence management process.

REFERENCES

- Shrutesh Jamulkar ,Preeti Chandrakar, Rifaqat Ali,Aman Agrawal, et. al., “Evidence Management System Using Blockchain and Distributed File System (IPFS)” published in research gate open

Access, available at

<https://www.researchgate.net/publication/354964804>.

- Ashitha C A, Asik Anwar M N,Fathima Shani, Rizwanul Haq, Chithra Rani P R, et. al., “Screening Forensic Evidence Employing Blockchain” published in ijsdr open Access, available at <https://www.ijsdr.org/papers/IJSDR2305294.pdf>.
- Karthik, Trishar T Suvarna, Karthik Shetty, U Ashvitha, et. al., “ENIGMA - A SECURE FORENSIC DATA SHARING USING BLOCKCHAIN ” published in ijeast open Access, available at <https://www.ijeast.com/papers/222-228.%20Tesma0703,IJEAST.pdf>.