

# CRIME DATA MANAGEMENT SYSTEM USING BLOCKCHAIN

<sup>1</sup>Dr.K.Balasubramanian, <sup>2</sup>Nithies.M, <sup>3</sup>Shithik Asath.M, <sup>4</sup>Vigneshwar.K

<sup>1</sup>Assistant Professor, <sup>2,3,4</sup> Final Year Student

<sup>1,2,3,4</sup> Department of Computer Science and Engineering

<sup>1,2,3,4</sup> E.G.S Pillay Engineering College, Nagapattinam, India

## ABSTRACT

The integrity and security of crime records and digital evidence are critical for effective law enforcement and judicial processes. Traditional crime data management systems suffer from significant challenges such as evidence tampering, unauthorized modifications, weak chain-of-custody tracking, and lack of transparent audit mechanisms. These limitations can compromise criminal investigations and reduce trust in the justice system. To address these issues, this research proposes a Blockchain-Based Crime Data and Digital Evidence Management System designed for law enforcement agencies and judicial institutions in India.

The proposed system leverages Ethereum blockchain technology to ensure immutable and tamper-proof storage of crime records, while IPFS (InterPlanetary File System) is used for decentralized storage of digital evidence such as images, videos, documents, and forensic reports. Smart contracts written in Solidity enforce role-based access control and maintain an auditable log of all transactions, ensuring accountability and transparency. The system architecture integrates a Node.js and Express backend for authentication, authorization, and API services, along with a React.js and Tailwind CSS frontend that provides secure role-based dashboards for police officers, forensic experts, administrators, and court officials.

The platform enables secure FIR registration, evidence upload, forensic verification, and chain-of-custody tracking using cryptographic hashes and digital signatures through MetaMask. Experimental evaluation demonstrates improved evidence integrity, enhanced transparency, and resistance to unauthorized data manipulation compared to conventional systems.

The proposed solution highlights the potential of blockchain technology in strengthening digital evidence management, improving judicial reliability, and promoting transparency and accountability within the criminal justice ecosystem.

## I. INTRODUCTION

Crime data management plays a crucial role in modern law enforcement and judicial systems. Law enforcement agencies generate and manage a vast amount of sensitive information, including First Information Reports (FIRs), investigation records, digital evidence, forensic reports, and case documentation. Maintaining the integrity, security, and traceability of this data is essential for ensuring fair investigations and reliable judicial outcomes.

Traditional crime data management systems are generally centralized and controlled by a single authority. Although these systems enable digital record storage and retrieval, they are vulnerable to several issues such as unauthorized access, data tampering, lack of transparency, and weak chain-of-custody tracking. In some cases, evidence may be altered, deleted, or manipulated, which can compromise criminal investigations and weaken legal proceedings. These limitations reduce the reliability of digital records and may affect public trust in law enforcement institutions. With the advancement of blockchain technology, new opportunities have emerged to address these challenges.

Blockchain is a decentralized and distributed ledger technology that records transactions securely across multiple nodes. Each transaction is cryptographically linked to the previous one, creating an immutable chain of records. Once data is stored on the blockchain, it cannot be modified or deleted, ensuring high levels of transparency, integrity, and accountability.

This project proposes a Blockchain-Based Crime Data and Digital Evidence Management System designed to enhance the security and reliability of crime-related records. The system uses blockchain technology to create tamper-proof records for case data and evidence logs, while decentralized storage mechanisms are used to store large digital evidence files. Smart contracts are utilized to enforce role-based access control, ensuring that only authorized personnel such as police officers, forensic experts, administrators, and judicial authorities can access or update specific records.

By integrating blockchain technology into crime data management, the proposed system ensures secure evidence tracking, transparent audit trails, and reliable chain-of-custody management. This approach significantly reduces the risk of data manipulation and enhances trust among law enforcement agencies, judicial authorities, and the public.

## II. LITERATURE SURVEY

Several researchers have explored technological approaches to improve the security, transparency, and reliability of crime data management and digital evidence handling systems. The major approaches are summarized below.

### A. Traditional Crime Data Management Systems

Most existing crime data management systems used by law enforcement agencies rely on centralized databases to store criminal records, investigation reports, and digital evidence. Although these systems allow efficient storage and retrieval of information, they face several challenges such as unauthorized access, data tampering, lack of transparency, and weak audit mechanisms. Since the data is controlled by a single authority, it becomes vulnerable to manipulation, which may compromise criminal investigations and judicial outcomes.

### B. Blockchain-Based Security Systems

Blockchain technology has been widely studied for its ability to provide secure and decentralized data management. It uses a distributed ledger system where each transaction is recorded in a block and linked to the previous block through cryptographic hashing. This structure ensures that once data is stored, it cannot be altered or deleted without network consensus. Researchers have proposed blockchain-based frameworks for secure record management, identity verification, and digital evidence tracking due to its tamper-proof and transparent nature.

### C. Smart Contract-Based Access Control

Smart contracts are programmable scripts deployed on blockchain networks that automatically execute predefined conditions. In crime data management systems, smart contracts can be used to enforce role-based access control and maintain an immutable log of system activities. They can ensure that only authorized personnel such as police officers, forensic analysts, and judicial authorities are allowed to access or submit case-related data. This automated enforcement reduces the risk of unauthorized data manipulation.

Recent studies indicate that integrating blockchain technology with crime data and digital evidence management systems significantly improves transparency, traceability, and security. The use of decentralized storage, cryptographic verification, and immutable audit trails helps maintain the integrity of criminal records and strengthens trust in law enforcement and judicial processes.

## III. PROBLEM STATEMENT

Traditional crime data management systems face several challenges that affect the security, transparency, and reliability of criminal investigations.

- Risk of evidence tampering or unauthorized modification of digital records
- Dependence on centralized databases controlled by a single authority
- Lack of transparent audit trails for tracking access and updates to case data
- Weak chain-of-custody management for digital evidence
- Difficulty verifying the authenticity and integrity of stored crime records

These limitations highlight the need for a secure and decentralized system that ensures transparency, accountability, and reliable evidence management. A blockchain-based solution can provide immutable records, cryptographic

verification, and transparent audit trails, enabling law enforcement agencies and judicial authorities to securely manage crime data and digital evidence while preventing unauthorized modifications.

#### IV. OBJECTIVES

The primary objectives of this project include:

1. Develop a secure crime data management system using blockchain technology.
2. Ensure tamper-proof storage of crime records and digital evidence.
3. Maintain transparent and immutable audit trails for all system activities.
4. Implement smart contracts to enforce role-based access control and data integrity.
5. Enable secure storage and verification of digital evidence using decentralized technologies.
6. Provide a user-friendly web interface for police officers, forensic experts, administrators, and judicial authorities.
7. Improve transparency, accountability, and trust in law enforcement and judicial processes.

#### V. PROPOSED METHODOLOGY

The proposed system integrates blockchain technology with a secure web application to create a transparent and tamper-proof crime data and digital evidence management platform.

##### Step 1 – User Registration

Authorized users such as police officers, forensic experts, administrators, and court officials create accounts on the system. Each user is assigned a specific role and connects their blockchain wallet for secure authentication and transaction verification.

##### Step 2 – FIR and Case Registration

Police officers register new criminal cases by entering FIR details and case information into the system. Each case is assigned a unique identifier and the basic case data is recorded securely.

##### Step 3 – Evidence Upload

Digital evidence such as images, videos, documents, and audio files are uploaded to decentralized storage. A cryptographic hash of the evidence is generated and stored on the blockchain to ensure integrity and authenticity.

##### Step 4 – Blockchain Recording

All important actions such as case registration, evidence submission, and forensic verification are recorded on the blockchain ledger. This ensures that the records are immutable, transparent, and tamper-proof.

##### Step 5 – Monitoring and Verification

Authorized users can monitor case progress, verify digital evidence through hash comparison, and access secure audit logs through the web interface. Judicial authorities can also verify the authenticity of evidence during legal proceedings.

#### VI. SYSTEM ARCHITECTURE

The proposed system follows a layered architecture consisting of four main components to ensure secure, transparent, and efficient management of crime data and digital evidence.

- **Presentation Layer** – The user interface built using modern web technologies allows authorized users such as police officers, forensic experts, administrators, and court officials to interact with the system. It provides role-based dashboards for case registration, evidence submission, and verification.
- **Application Layer** – This layer handles user authentication, role-based access control, case management, and evidence processing. It manages the communication between the user interface and the blockchain network while ensuring that only authorized users can perform specific actions.

- **Blockchain Layer** – Smart contracts deployed on the Ethereum blockchain manage the secure recording of case data and evidence hashes. All important actions such as case creation, evidence submission, and verification are stored as immutable blockchain transactions.
- **Storage Layer** – Decentralized storage solutions such as IPFS store large digital evidence files including images, videos, documents, and forensic reports. The cryptographic hash of each file is recorded on the blockchain to ensure data integrity and tamper-proof verification.

## VII. FLOW DIAGRAM

The operational workflow of the system includes the following steps:

1. Authorized user registers and logs into the platform.
2. Police officers register a new case or FIR in the system.
3. Digital evidence such as images, videos, or documents is uploaded to the system.
4. The evidence file is stored in decentralized storage and a cryptographic hash is generated.
5. Smart contracts record the evidence hash and case details on the Ethereum blockchain.
6. The blockchain ledger permanently stores the case and evidence records ensuring immutability.
7. Authorized authorities can verify evidence integrity and monitor case progress through the platform.

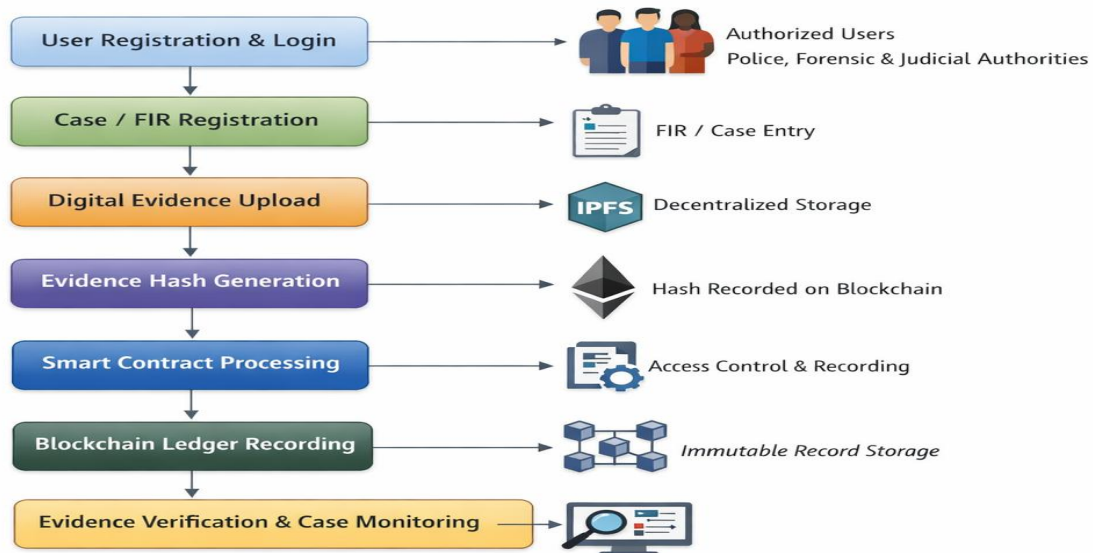


figure 1

## VIII. HARDWARE DESIGN

Since the proposed system is a web-based blockchain platform for crime data and digital evidence management, it mainly depends on computing infrastructure rather than specialized hardware components.

### A. User Devices

Authorized users such as police officers, forensic experts, administrators, and judicial authorities access the system using computers, laptops, tablets, or secure mobile devices to manage cases and evidence.

## **B. Blockchain Network**

Blockchain nodes maintain the distributed ledger and validate transactions related to case registration, evidence submission, and verification on the Ethereum network.

## **C. Server Infrastructure**

Backend servers handle application logic, user authentication, role-based access control, and communication between the web application, blockchain network, and decentralized storage systems.

## **D. Internet Connectivity**

Reliable internet connectivity is required for users to access the platform, upload digital evidence, and perform blockchain transactions securely across the network.

## **IX. SOFTWARE DESIGN**

The system software consists of multiple components working together to support secure crime data and digital evidence management.

- Frontend Interface – A web-based user interface developed using modern web technologies to allow police officers, forensic experts, administrators, and court officials to interact with the system.
- Backend Server – The backend server handles user authentication, role-based access control, case management, and communication between the application and blockchain network.
- Smart Contracts – Smart contracts written in Solidity manage the secure recording of case details, evidence hashes, and access permissions on the blockchain.
- Blockchain Development Framework – A blockchain development environment such as Truffle is used for deploying, testing, and managing smart contracts on the Ethereum network.
- Integration Libraries – Libraries such as Web3.js enable communication between the web application and the blockchain network for executing transactions and retrieving blockchain data.

These components work together to provide a secure, transparent, and efficient platform for managing crime data and digital evidence.

## **X. WORKING**

The Blockchain-Based Crime Data Management System operates by connecting law enforcement authorities, forensic experts, and judicial officials through a secure web-based application integrated with blockchain infrastructure.

When a police officer registers a new case or uploads digital evidence, the request is processed through the system and the evidence file is stored in decentralized storage. A cryptographic hash of the evidence is generated and sent to the Ethereum network. A smart contract verifies the transaction details and records the evidence hash along with case information on the blockchain ledger. Once the transaction is confirmed, the system updates the case record and securely maintains the chain of custody.

The platform also provides role-based dashboards where authorized users can view case details, evidence records, and blockchain transaction hashes. Forensic experts can verify the integrity of evidence through hash comparison, while judicial authorities can review the immutable audit trail. This ensures transparency, prevents evidence tampering, and allows authorities to verify the authenticity and history of digital evidence throughout the investigation process.

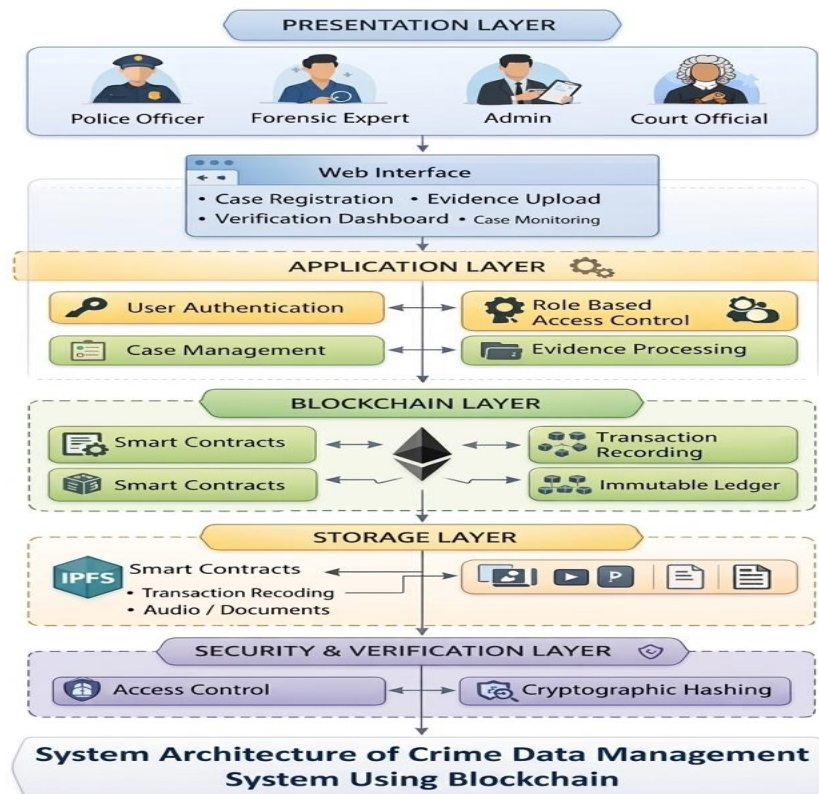


figure 2

## XI. ADVANTAGES

The proposed Crime Data Management System Using Blockchain offers several advantages compared to traditional crime record management systems.

- Provides transparency through immutable blockchain transaction records for case data and evidence handling.
- Prevents evidence tampering by storing cryptographic hashes of digital evidence on the Ethereum network.
- Maintains a secure chain of custody for digital evidence throughout the investigation process.
- Improves accountability by recording every action in a permanent and auditable blockchain ledger.
- Ensures secure and tamper-proof storage of digital evidence using decentralized systems like IPFS.
- Enhances trust between law enforcement agencies, forensic departments, and judicial authorities through transparent evidence verification.

## XII. APPLICATIONS

The proposed Crime Data Management System Using Blockchain can be applied in multiple domains where secure and tamper-proof crime record management is essential.

- Law Enforcement Agencies for secure storage and management of FIR records, investigation data, and digital evidence.
- Forensic Departments for verifying and analyzing digital evidence while maintaining a proper chain of custody.
- Judicial Systems and Courts for verifying the authenticity and integrity of evidence during legal proceedings.
- Cybercrime Investigation Units for securely managing digital crime records and electronic evidence.
- Government Crime Record Bureaus for maintaining transparent and tamper-proof criminal databases.

By implementing blockchain technology using platforms like Ethereum, the system can significantly improve security, transparency, and reliability in crime data management.

### XIII. FUTURE ENHANCEMENTS

Several enhancements can further improve the capabilities of the proposed Crime Data Management System Using Blockchain.

- Integration with multiple blockchain networks to improve scalability and interoperability of crime data management systems.
- Implementation of advanced analytics to analyze crime patterns and assist law enforcement agencies in decision making.
- Integration with national crime databases to enable secure sharing of crime records between different law enforcement departments.
- AI-based crime analysis to detect suspicious patterns, predict criminal activities, and support investigation processes.
- Mobile application development to allow authorized officers to securely access and update crime records from field locations.

### REFERENCES

- [1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
- [2] Melanie Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, 2015.
- [3] Michael Crosby, Pradan Pattanayak, Sanjay Verma, and Vignesh Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, 2016.
- [4] Gavin Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," *Ethereum Project Yellow Paper*, 2014.
- [5] Don Tapscott and Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, Penguin Random House, 2016.

#### Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.