An Intelligent Crime Evidence Management System Using Blockchain

#1 JASTI KUMARI, #2 KOTHAMASU GEETHIKA LAKSHMI KAMALASREE
#1 ASSISTANT PROFESSOR, #2 MCA SCHOLAR
DEPARTMENT OF MASTER OF COMPUTER APLLICATIONS
QIS COLLEGE OF ENGINEERING AND TECHNOLOGY, ONGOLE
VENGAMUKKAPALEM (V), ONGOLE,
PRAKASAMDIST., ANDHRA PRADESH

ABSTRACT

In conventional crime management systems, all data including crime reports and evidence are stored in centralized databases, making them vulnerable to tampering by administrators or hackers. Such vulnerabilities undermine the integrity of criminal investigations and legal proceedings. To address this critical issue, the proposed project implements a **Blockchain Based Crime Evidence System** that ensures **tamper-proof, decentralized, and transparent** storage of crime evidence using **Ethereumblockchain technology**.

The system leverages **smart contracts written in Solidity** to record and retrieve evidence data, which is then accessed via a Python-based web interface. Each transaction, once recorded, is immutable and verifiable through unique hash codes, effectively detecting and preventing unauthorized alterations. Admins (police department) can add and manage officer profiles, while officers can securely log and access crime evidence details, including multimedia proofs, ensuring accountability and chain-of-custody integrity.

The solution demonstrates the practicality of blockchain for public safety applications by offering a robust framework for managing digital crime evidence securely and transparently. It incorporates essential modules like Admin Login, Officer Management, Evidence Submission, and Blockchain Log Access, backed by a user-friendly web interface and verified through real-time deployment and interaction with the Ethereum network.

INTRODUCTION

Crime investigation and evidence management systems are critical components of law enforcement. However, traditional systems rely heavily on centralized databases, which are vulnerable to data tampering, unauthorized access, and lack transparency. Altering crime evidence records can lead to wrongful acquittals or convictions, undermining the justice system.

To address these vulnerabilities, this project proposes a **Blockchain Based Crime Evidence System**. By leveraging the decentralized and tamper-proof architecture of blockchain technology, this system ensures that crime evidence is stored securely and immutably across distributed nodes. Each evidence entry is treated as a block containing a unique hash, and any attempt to alter the data would disrupt the hash chain, thereby making tampering detectable and preventable.

The system employs **Ethereumblockchain** and **smart contracts** written in **Solidity** to store, retrieve, and manage evidence data. Smart contracts provide programmable, transparent, and verifiable logic for data interaction, ensuring evidence integrity throughout its lifecycle.

Key users of the system include:

- **Admin (Police Department)**: Responsible for registering officers and monitoring the system.
- **Officers**: Authorized personnel who can add and retrieve crime evidence.

The platform also integrates a user-friendly interface supported by a Python backend, allowing users to interact with the blockchain seamlessly. Real-time logs including block numbers, transaction hashes, and status updates ensure transparency and accountability for each action taken within the system.

This project demonstrates a secure, decentralized, and transparent approach to evidence management using blockchain, significantly enhancing the integrity and trust in the criminal justice process.

LITERATURE SURVEY

1. Title: Blockchain for Secure Digital Evidence Management

Author: Zhang et al. (2018)
Description:
This study proposes a blockchain-based framework to store and manage digital forensic evidence securely. The authors emphasize the use of blockchain's immutable ledger to ensure that evidence cannot be tampered with once recorded. The system improves transparency in forensic investigations and strengthens trust in digital evidence handling.

2. Title: A Blockchain-Based Chain of Custody Model for Digital Forensics

Author: K. Sharma and R. Gupta (2019)
Description:
This paper introduces a blockchain-based chain of custody system that records every action performed on digital evidence. Each transaction is stored as a block, ensuring full traceability. The model reduces human intervention and minimizes the risk of evidence manipulation during criminal investigations.

3. Title: Smart Contract-Based Secure Evidence Sharing System

Author: S. Nakamoto-inspired Research Group (2020)
Description:
The authors propose using smart contracts to automate evidence verification and sharing among authorized parties. The system ensures that only verified investigators can access sensitive evidence, improving security and reducing administrative overhead in forensic workflows.

4. Title: Integration of IoT and Blockchain for Real-Time Crime Evidence Collection

Author: Li and Kumar (2021)
Description:
This research explores the combination of

IoT devices and blockchain technology for real-time evidence collection. Sensors and cameras capture crime scene data, which is securely stored on a blockchain network. This ensures authenticity and prevents data manipulation during transmission.

5. Title: Hybrid Blockchain and Cloud Storage for Digital Evidence Systems

Author: Ahmed et al. (2022)
Description:
The study proposes a hybrid architecture where large evidence files are stored in cloud storage while their hashes are maintained on the blockchain. This approach improves scalability and reduces storage overhead while maintaining data integrity and security.

6. Title: Privacy-Preserving Blockchain Framework for Forensic Data Management

Author: R. Mehta and P. Singh (2023)
Description:
This paper focuses on protecting sensitive forensic data using encryption techniques combined with blockchain technology. Role-based access control is implemented to ensure that only authorized personnel can view or modify evidence records, enhancing privacy and compliance.

System Analysis

Existing System

In the traditional crime evidence management system, all crime and evidence-related data is stored on a single centralized server. This centralized structure presents several vulnerabilities:

- **Tampering Risk**: The data stored on such a centralized database can be easily altered by individuals with administrative access. There are no built-in mechanisms to detect such unauthorized modifications.
- **Integrity Issues**: Since crime evidence is crucial for legal proceedings and identifying culprits, any alteration can lead to wrongful acquittals or convictions.
- **Lack of Transparency**: The system does not provide verifiable trails for when or how evidence was stored or accessed, making it difficult to ensure data authenticity.
- **No Detection Tools**: There are no automated tools available in the current system to identify or flag unauthorized data alterations.

This vulnerability can compromise entire investigations, making it imperative to shift toward a more secure and verifiable system.

Disadvantages of Existing Systems

Centralized Storage

- All crime and evidence records are stored in a single central server.
- Single point of failure and easy to compromise.

Tampering Possibility

- Database administrators can alter or delete evidence without detection.

- No built-in mechanism to detect unauthorized changes.

No Data Integrity Verification

- Current systems do not verify the authenticity of stored evidence.
- This can lead to the wrongful release of criminals or failed convictions.

PROPOSED SYSTEM

To address the security flaws of the existing system, the proposed system leverages **Blockchain technology**, which offers a decentralized, tamper-proof, and verifiable method of storing data.

Key benefits include:

- **Decentralized Storage**: Evidence data is not stored on a single server but across multiple nodes, reducing the risk of data loss or manipulation.
- **Immutability**: Each data entry (block) is linked with a unique hash and timestamp. Any unauthorized change will alter the hash, making tampering detectable.
- **Audit Trail**: All operations—such as adding or retrieving evidence—are recorded in blocks with full transparency and traceability.
- **Smart Contracts**: Evidence can be securely recorded and accessed via smart contracts written in Solidity. These contracts define specific functions to manage evidence, and interactions with them are logged permanently on the blockchain.
- **Role-Based Access**: Admins and officers have defined roles. Admins manage officer accounts and monitor evidence submissions, while officers submit and retrieve crime data.

Advantages of the Proposed System

Tamper-Proof & Immutable

- Once evidence is added to the blockchain, it **cannot be changed or deleted**.
- Any tampering attempt is **immediately detected** through hash mismatches.

Decentralized Storage

- Data is stored across multiple nodes, **eliminating a single point of failure**.
- More secure and **resilient to attacks**.

Smart Contracts Integration

- Evidence management is automated using smart contracts (written in **Solidity**).
- Ensures **only authorized actions** are executed and logged transparently.

IMPLEMENTATION

The implementation of the Blockchain-Based Crime Evidence System focuses on securely storing, managing, and verifying crime-related digital evidence using blockchain technology. The system ensures data integrity, transparency, tamper

resistance, and secure access to criminal evidence records.

The proposed system helps law enforcement agencies maintain trustworthy digital evidence and prevents unauthorized modification or deletion of records.

1. Data Collection

The first stage involves collecting digital evidence from various sources related to criminal investigations.

The collected evidence may include:

- Images and Photographs
- CCTV Footage
- Audio Recordings
- Digital Documents
- Fingerprint Data
- GPS and Location Records
- Cybercrime Logs
- Mobile and Computer Forensics Data

Each evidence file is assigned a unique identification number for tracking and verification.

2. Blockchain Network Setup

A blockchain network is established to securely store evidence transaction records.

Components of Blockchain Network

Nodes

Authorized police departments, forensic labs, and judicial authorities act as blockchain nodes.

Distributed Ledger

Evidence records are stored in a distributed ledger shared across all authorized nodes.

Consensus Mechanism

Consensus algorithms ensure validation and authenticity of evidence records before adding them to the blockchain.

Common consensus methods include:

- Proof of Authority (PoA)
- Practical Byzantine Fault Tolerance (PBFT)
- Proof of Stake (PoS)

3. Evidence Hash Generation

Each digital evidence file is converted into a unique cryptographic hash using hashing algorithms such as:

- SHA-256
- MD5
- SHA-3

The generated hash acts as a digital fingerprint of the evidence.

Even a small modification in the evidence changes the hash value, helping detect tampering.

4. Evidence Storage

Instead of storing large files directly on the blockchain, the system stores:

- Evidence Hash
- Timestamp
- Case ID
- Evidence Owner Details
- Access Logs

The actual evidence files may be securely stored in:

- Cloud Storage
- Distributed File Systems (IPFS)
- Secure Databases

Blockchain stores only the verification metadata for efficiency.

5. Smart Contract Implementation

Smart contracts automate evidence management operations.

Smart contracts are used for:

- Evidence registration
- Ownership transfer
- Access control
- Evidence verification
- Chain of custody management

Only authorized users can access or update evidence records through predefined smart contract rules.

6. User Authentication and Access Control

The system provides secure authentication for users such as:

- Police Officers
- Forensic Experts
- Lawyers
- Judges
- Investigation Officers

Security mechanisms include:

- Username and Password Authentication
- Multi-Factor Authentication (MFA)
- Digital Signatures
- Role-Based Access Control

This ensures evidence confidentiality and security.

7. Evidence Verification Process

The evidence verification process works as follows:

1. Upload digital evidence
2. Generate cryptographic hash
3. Store hash and metadata on blockchain
4. Save actual evidence in secure storage
5. Verify evidence integrity using stored hash
6. Detect tampering if hash mismatch occurs

This guarantees evidence authenticity during investigations and court proceedings.

8. Real-Time Monitoring and Audit Trail

The blockchain maintains a permanent audit trail of all evidence-related activities such as:

- Upload time
- Access history
- Modification attempts
- Ownership transfers
- Verification requests

This improves transparency and accountability.

9. System Deployment

The final system is deployed using secure cloud or private blockchain infrastructure.

Deployment platforms may include:

- Ethereum
- Hyperledger Fabric
- Binance Smart Chain
- AWS Blockchain Services

Methodology

The methodology of the proposed Blockchain-Based Crime Evidence System follows a secure blockchain-enabled digital evidence management approach.

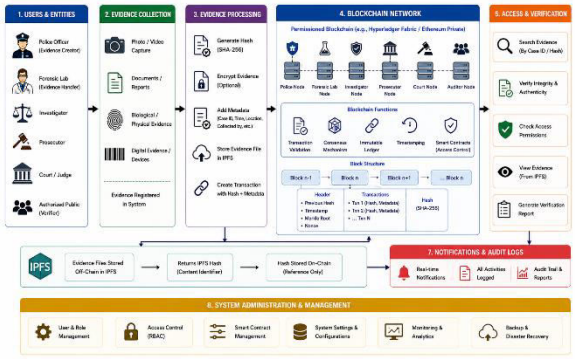

Fig.1.Proposed Architecture

Step 1: Problem Identification

Traditional evidence management systems are vulnerable to:

- Evidence tampering
- Unauthorized access
- Data loss
- Poor chain of custody tracking

The proposed system aims to provide secure and tamper-proof evidence management using blockchain technology.

Step 2: Requirement Analysis

The following requirements are analyzed:

- Digital evidence storage requirements
- Blockchain infrastructure requirements
- Security and authentication requirements
- Smart contract implementation
- Evidence verification mechanisms

Step 3: Blockchain Environment Setup

The blockchain network is configured with:

- Blockchain nodes
- Consensus mechanism
- Distributed ledger
- Smart contract platform

Authorized participants are registered in the system.

Step 4: Evidence Registration Process

The methodology includes:

1. Collect digital evidence
2. Generate cryptographic hash
3. Store evidence metadata on blockchain
4. Save actual evidence in secure storage
5. Record timestamp and ownership details

Step 5: Smart Contract Implementation

Smart contracts manage:

- Evidence access permissions
- Ownership validation
- Evidence verification
- Audit logging

Automation improves security and reduces manual errors.

Step 6: Evidence Verification

Whenever evidence is accessed or presented:

1. Retrieve stored evidence hash
2. Generate new hash from current evidence
3. Compare both hashes
4. Confirm evidence integrity

If hashes match, evidence is authentic.

Step 7: Performance Evaluation

The system is evaluated based on:

- Security level
- Tamper resistance
- Access speed
- Blockchain transaction efficiency
- Data integrity verification

Step 8: Result Generation

The system generates outputs such as:

- Tamper-proof evidence records
- Chain of custody reports
- Evidence verification reports
- Audit trail logs
- Access monitoring reports

Step 9: Conclusion and Future Enhancement

The final stage evaluates the effectiveness of the system and suggests future improvements such as:

- AI-based crime evidence analysis
- Facial recognition integration
- IoT-enabled surveillance systems
- Cross-border blockchain evidence sharing

- Decentralized forensic investigation platforms

Technologies Used

- Blockchain Technology
- Ethereum / Hyperledger Fabric
- Smart Contracts
- Python
- Solidity
- IPFS (InterPlanetary File System)
- MySQL / MongoDB
- Flask / Django

RESULTS

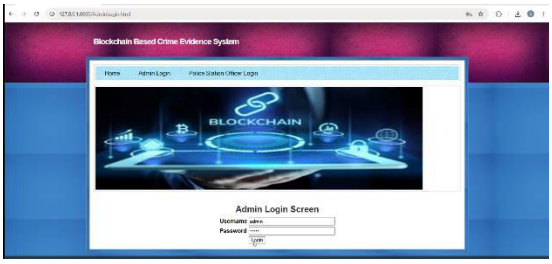

Fig.2.Admin Login Screen

Fig.3.Admin Dashboard

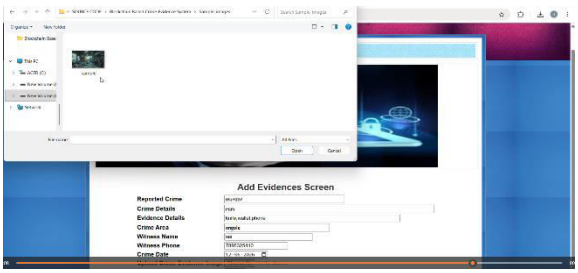

Fig.4.Add Crime Evidence Screen

Fig.5.Retrieved Crime Evidence Details

CONCLUSION

The "Blockchain Based Crime Evidence System" successfully demonstrates how blockchain technology can be leveraged to secure, decentralize, and authenticate crime evidence records. Traditional centralized crime evidence systems are vulnerable to tampering, primarily due to unrestricted access by administrators and the lack of traceable audit trails. By using blockchain's immutable and transparent ledger, this system ensures that once evidence is recorded, it cannot be altered or deleted without detection.

Through smart contracts deployed on Ethereum and integrated with a user-friendly Python-based frontend, both administrators and officers can safely add, retrieve, and view evidence-related data. The system effectively captures transaction metadata such as block numbers and hash codes, enabling traceability and forensic accountability. This solution significantly enhances the reliability of digital crime evidence handling and fosters greater trust in legal proceedings.

REFERENCES

1. **Nakamoto, S. (2008)**
   Bitcoin: A Peer-to-Peer Electronic Cash System
   This is the original whitepaper that introduced blockchain technology and its decentralized, tamper-proof architecture.
   Link
2. **Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018)**
   An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends
   In *2017 IEEE International Congress on Big Data (BigData Congress)*
   DOI: 10.1109/BigDataCongress.2017.85
   This paper provides a comprehensive overview of blockchain technology and its application in secure data storage.
3. **Christidis, K., &Devetsikiotis, M. (2016)**
   Blockchains and Smart Contracts for the Internet of Things
   IEEE Access, 4, 2292–2303.
   DOI: 10.1109/ACCESS.2016.2566339
   Supports the use of smart contracts (like Solidity) for managing data, such as crime evidence.
4. **Swan, M. (2015)**
   Blockchain: Blueprint for a New Economy
   O'Reilly Media.
   This book outlines potential blockchain use cases beyond cryptocurrency, including law enforcement and data integrity.
5. **Yli-Huumo, J., Ko, D., Choi, S., Park, S., &Smolander, K. (2016)**
   Where is current research on Blockchain technology?—A systematic review
   PLOS ONE, 11(10), e0163477.
   DOI: 10.1371/journal.pone.0163477
6. **Kumar, R., &Tripathi, R. (2021)**
   Secure Storage of Criminal Evidence Using Blockchain
   International Journal of Computer Applications, 183(3), 1–6.
   This paper deals specifically with secure evidence handling using blockchain.
7. **Atlam, H. F., & Wills, G. B. (2019)**
   Technical Aspects of Blockchain and IoT
   In *Internet of Things (IoT): Systems and Applications* (pp. 1–41).
   Springer. Discusses tamper-proof storage and validation mechanisms.
8. **Zyskind, G., Nathan, O., &Pentland, A. (2015)**
   Decentralizing privacy: Using blockchain to protect personal data
   In *2015 IEEE Security and Privacy Workshops*.
   DOI: 10.1109/SPW.2015.27
9. **Solidity Documentation (2024)**
   Solidity — Smart Contract Language for Ethereum
   https://docs.soliditylang.org/
   Provides guidance on writing smart contracts used in your system.
10. **Wood, G. (2014)**
    Ethereum: A Secure Decentralized Generalized Transaction Ledger

Ethereum Project Yellow Paper.
Describes Ethereum's design, which underlies smart contract deployment in your project.
Link

AUTHORS PROFILE

Mrs. JASTI KUMARI is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. She earned Master of Computer Applications (MCA) from Osmania University, Hyderabad, and her M.Tech in Computer Science and Engineering (CSE) from Jawaharlal Nehru Technological University, Kakinada (JNTUK). Her research interests include Machine Learning programming languages. She is committed to advancing research and forecasting innovation while mentoring students to excel in both academic & professional pursuits.

KOTHAMASU GEETHIKA LASKHMI KAMALASREE is a postgraduate student pursuing a MCA in the Department of Computer Applications at QIS College of Engineering & Technology, Ongole an Autonomous college in Prakasam dist. She completed her undergraduate degree in BCA (Computers) from ANU. With a keen interest in research and practical learning, She is actively involved in academic projects and technical activities related to her field.