IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 4, June 2025

Impact Factor: 7.67

Evidence Protection and Assisting Police using Blockchain

Randive Prem[1], Mangesh Javanjale[2], Abhishek Narnavale[3], G. T. Avhad[4]

Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar,India[1,2,3]

Professor, Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Pune, India[4]

Abstract: *The dependence on digital evidence in the justice system is growing rapidly, highlighting the urgent requirement for systems that are secure, efficient, and resistant to tampering. This study introduces a blockchain-integrated evidence management system designed to enhance the authenticity, reliability, and traceability of digital evidence. By utilizing blockchain's decentralized ledger technology, the system records evidence interactions such as submissions and access events, ensuring immutability and transparency. It addresses several drawbacks in conventional systems, such as vulnerability to tampering, manual inefficiencies, and inconsistent documentation. This innovative framework empowers law enforcement to maintain reliable digital trails, boosting public confidence and trust in judicial processes..*

Keywords: Blockchain, Digital Evidence, Chain of Custody, Law Enforcement, Evidence Tracking

I. INTRODUCTION

In contemporary criminal investigations and court processes, the accuracy and safety of digital evidence are paramount. Traditional evidence handling techniques often lack proper tracking and are vulnerable to unauthorized access or manipulation, particularly when dealing with growing volumes of electronic data. These limitations threaten the credibility and admissibility of digital proof.

This paper presents a blockchain-based evidence system engineered to address these deficiencies. Blockchain's decentralized and immutable ledger provides a transparent record of every interaction with evidence, fortified by time-stamped entries. Smart contracts automate the regulation of access rights, restricting evidence visibility and modification exclusively to approved users. Additionally, scalable cloud infrastructure supports efficient data storage, while strong encryption safeguards sensitive content.

This proposed model offers a significant advancement over outdated manual systems, aiming to support more dependable legal outcomes and to streamline forensic procedures. It establishes a new paradigm for digital evidence security, aligning law enforcement efforts with cutting-edge technological trends.

II. LITERATURE REVIEW

[1]Blockchain in Forensic Management:

Blockchain's immutability and decentralization have proven useful in forensic evidence storage. Each item is cryptographically hashed and entered into a distributed ledger. Smart contracts further automate verification, though concerns around scalability and legal integration persist.

[2] IoT-Based Forensics with Fuzzy Hashing:

By combining fuzzy hashing with blockchain in an IoT framework, digital forensic systems gain resilience against data distortion. However, these implementations require considerable resources and complex infrastructure.

[3] Blockchain for IoT Evidence Collection:

Timestamped data from IoT devices stored immutably on blockchain improves data integrity and accessibility. Nevertheless, scalability, training, and cost factors pose adoption challenges**.**

DOI: 10.48175/568

[4] IPFS and Blockchain for Evidence Storage:
The blend of IPFS with blockchain enhances decentralization and tamper resistance in evidence management. Although effective, issues such as file volume, implementation complexity, and legal compliance remain.

[5] **Forensic-Chain using Hyperledger:**
Hyperledger Composer-based solutions offer detailed audit trails and tamper-proof chains of custody. Despite the security benefits, these systems demand specialized skills and adaptation to legacy forensic tools.

[6] Hyperledger Fabric in Digital Evidence Systems:
Permissioned blockchain networks like Hyperledger Fabric enable secure, timestamped evidence tracking with automated control using smart contracts. These systems enhance access control but require expertise and investment.

[7] Integrated Forensic Frameworks:
Proposing unified models across forensic stages promotes collaboration and reduces redundancy. Widespread adoption, however, is hindered by rapid technological change and resistance to new standards.

III. METHODOLOGY OF PROPOSED SURVEY

Requirement Analysis

The system is designed with the following functional goals:

- Secure uploading of digital evidence (e.g., documents, images, videos).
- Controlled access through an intuitive user interface restricted to verified users.
- Blockchain registration with time stamps and cryptographic hashes to ensure data integrity.
- Smart contracts for enforcing access control.
- Immutable chain of custody for every evidence-related interaction.
- Automated audit trails and sharing capabilities.
- Real-time alerts for any unauthorized access attempts.

Non-functional requirements include:

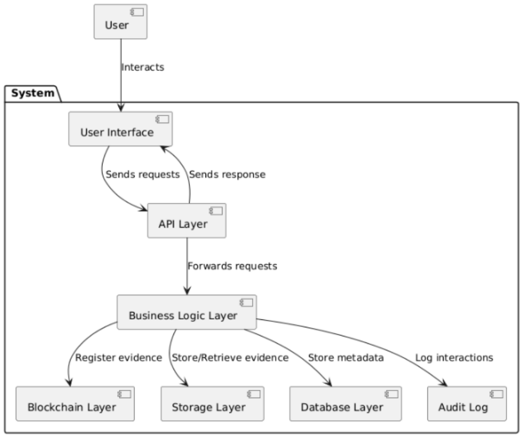
- High scalability and encryption standards.
- Responsive performance for upload/view tasks.
- Legal compliance with frameworks like GDPR and HIPAA.
- Minimal training needs due to a user-friendly interface.
- Reliable uptime and audit-ready logs.

IV. SYSTEM ARCHITECTURE

The architecture comprises the following layers:

- Frontend (UI): Built using React.js to facilitate secure and simple evidence interaction.
- API Layer: Manages HTTP/HTTPS requests between frontend and backend.
- Business Logic: Handles authentication, blockchain communication, access control, and data operations.
- Blockchain Layer: Maintains tamper-proof logs and smart contract-based access rights.
- Storage Layer: AWS cloud services store large digital evidence securely.
- Database Layer: A NoSQL MongoDB database stores metadata and supports unstructured data management.
- Audit & Logs: The ELK Stack is used for tracking user activities and generating compliance reports.
- Alert System: Monitors and notifies administrators of unauthorized attempts.

DOI: 10.48175/568



Data Flow Overview

- Users submit or retrieve evidence through the UI.
- Requests pass to the API Layer, which communicates with the Business Logic.
- Uploaded files are saved to the Storage Layer; metadata is stored in the Database Layer.
- Blockchain Layer records time-stamped, immutable transaction logs.
- Audit Logs are captured for all events.
- The system returns status updates to users and generates alerts for suspicious activity.

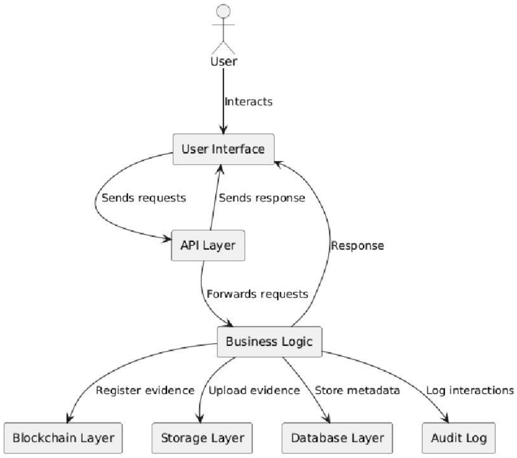


Fig. Data Flow Diagram

TECHNOLOGY STACK

- **Frontend:** React.js, HTML, CSS, JavaScript
- **Backend:** Node.js with Express.js
- **Blockchain Platform:** For smart contract and ledger functionality
- **Database:** MongoDB (NoSQL)
- **File Storage:** AWS Cloud and local storage during development
- **Security:** JWT for authentication; AES and RSA for encryption
- **Development Tools:** GitHub, Visual Studio
- **Monitoring Tools:** ELK Stack for logging and system monitoring

IV. CONCLUSION AND FUTURE WORK

The development of this blockchain-enabled evidence management system reflects the growing importance of secure, transparent, and tamper-proof solutions in modern law enforcement. The integration of smart contracts, cloud storage, and audit systems ensures legal robustness, high performance, and compliance with data privacy laws.

Initial testing has confirmed the system's effectiveness in fulfilling both functional and non-functional requirements. Moving forward, the system will be fine-tuned based on user feedback, with plans to explore AI-based analysis of digital evidence. Larger-scale deployments and further innovations will continue to evolve this platform, reinforcing its contribution to digital justice systems.

REFERENCES

[1]. Yan wu , Fang Lu Lu , "A Bitcoin Transaction Network Analysis Method for Future Blockchain Forensic Investigation"-2023

[2]. M. Sharma et al., "LoED: LoRa and edge computing based system architecture for sustainable forest monitoring," Int. J. Eng. Trends Technol., vol. 70, no. 5, pp. 88–93, 2022

[3]. D. Singh, R. Singh, A. Gehlot, S. V. Akram, N. Priyadarshi, and B. Twala, "An imperative role of digitalization in monitoring cattle health for sustainability," Electronics (Basel), vol. 11, no. 17, p. 2702, 2022

[4]. E. E.-D. Hemdan and D. H. Manjaiah, "An efficient digital forensic model for cybercrimes investigation in cloud computing," Multimed. Tools Appl., 2021.

[5]. Y. Maleh, and L. Tawalbeh, Artificial intelligence and blockchain for future cybersecurity applications, vol. 90. Springer Nature, 2021.

[6]. R. Sathyaprakasan, P. Govindan, S. Alvi, L. Sadath, S. Philip, and N. Singh, "An implementation of blockchain technology in forensic evidence management," in 2021

[7]. International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021

[8]. S. Patil, S. Kadam, and J. Katti, "Security enhancement of forensic evidences using blockchain," in 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021

[9]. Y. Baddi, M. Alazab "Forensic Evidence Security System using Blockchain Technology."- 2021

[10]. R. Singh et al., "Cloud server and Internet of Things assisted system for stress monitoring, Electronics (Basel), vol. 10, no. 24, p. 3133, 2021

DOI: 10.48175/568