IJMRSETM

e-ISSN: 2395 - 7639

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 12, Issue 5, May 2025

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.214

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 8.214 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 12, Issue 5, May 2025 |

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 increasing reliance on digital evidence in law enforcement and legal proceedings underscores the need for secure, efficient, and tamper-proof evidence management systems. This project presents a blockchain-based evidence management solution aimed at improving the integrity, traceability, and security of digital evidence. The system utilizes blockchain technology to create a decentralized, immutable ledger that records evidence submissions, access logs, and chain-of-custody information, ensuring transparency and authenticity. The proposed approach addresses the limitations of traditional evidence handling methods, such as tampering risks, inefficient manual processes, and inconsistent documentation practices. Through this innovative system, law enforcement agencies can significantly improve the accuracy and reliability of digital investigations, fostering trust and confidence in the judicial process.

KEYWORDS: Blockchain, Evidence management, Law enforcement, Digital evidence

I. INTRODUCTION

In modern law enforcement and judicial systems, the integrity, security, and traceability of digital evidence are critical to ensuring justice. The rapid increase in digital data used in crime investigations has highlighted significant limitations in traditional evidence management practices, which often rely on physical storage and manual processes prone to tampering, loss, and unauthorized access. These limitations compromise the credibility of evidence, potentially affecting the outcomes of legal proceedings. To address these challenges, this project proposes a blockchain-based evidence management system designed to revolutionize the handling of digital evidence. Blockchain technology offers a decentralized, tamper-proof ledger that records evidence transactions with time-stamped logs, ensuring data integrity and transparency. By integrating blockchain, the proposed system provides a reliable chain of custody and audit trails that can withstand reliability in court. Additionally, the system employs scalable cloud storage solutions for efficient evidence management and smart contracts to automate access control, restricting evidence viewing and modifications to authorized personnel only.The proposed solution not only reduces the risks associated with traditional evidence management but also aligns with advancements in digital technology to enhance law enforcement practices. Through this approach, the project aims to establish a secure, transparent, and efficient framework for digital evidence management, contributing to more effective crime-solving and increasing public confidence in the judicial process

II. LITERATURE REVIEW

[1] Implementation of Blockchain Technology in Forensic Evidence Management:

The approach to utilizing blockchain in forensic evidence management involves establishing a secure, decentralized, and non–tamperable system for storing digital evidence. It typically starts with setting up a distributed ledger, where each evidence item is given a unique cryptographic identifier and recorded as a transaction. This ledger, maintained by a network of nodes, ensures that no single entity controls the system. Smart contracts can automate the evidence verification process, enhancing the reliability and efficiency of forensic procedures. The use of cryptographic methods can protect sensitive information, improving transparency and traceability while reducing risks of evidence tampering. Challenges include scalability issues with certain blockchain networks and the need for legal considerations to align with established forensic practices.

[2] Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hashing:

This architecture combines IoT devices with blockchain technology, using fuzzy hashing to hash digital evidence in a way that tolerates slight data modifications. The hashed values are stored on a blockchain, ensuring their permanence and traceability. Smart contracts streamline the validation and verification processes, increasing tamper resistance and integrity in IoT digital forensics. The decentralized blockchain structure creates an auditable trail for evidence. However, potential challenges include implementation complexities, scalability limitations, and high resource requirements.

[3] IoT Forensics System Based on Blockchain:

Integrating IoT devices with blockchain technology for digital forensics involves collecting and timestamping evidence from IoT sources and storing it in an immutable ledger on the blockchain. This decentralized approach ensures the integrity of data while smart contracts automate evidence verification. The system enhances the security and transparency of forensic investigations by providing tamper-resistant evidence storage and improved traceability. However, challenges may arise in terms of scalability, adoption costs, and the need for training forensic professionals to use blockchain technology effectively.

[4] Combining Blockchain with IPFS for Crime Evidence Management:

This implementation uses blockchain alongside the InterPlanetary File System (IPFS) to create a tamper-proof record of crime evidence, with data linked to the IPFS network for decentralized file storage. The combination ensures the integrity, accessibility, and transparency of evidence management. The approach leverages blockchain's security and immutability while benefiting from IPFS's decentralized storage. Challenges include scalability issues due to large volumes of evidence files, implementation costs, and legal considerations for integrating with crime management systems.

[5] Forensic-Chain: Blockchain-Based Digital Forensics Chain of Custody Using Hyperledger Composer:

The Forensic-Chain framework establishes a decentralized, unchangeable ledger for managing the digital forensics chain of custody, implemented with a Proof of Concept (PoC) using Hyperledger Composer. Each forensic item is uniquely identified, and transactions are recorded on the blockchain to ensure a tamper-resistant and auditable custody trail. Benefits include enhanced security and transparency thanks to blockchain's decentralized features and Hyperledger Composer's tailored capabilities. Challenges involve requiring specialized knowledge of Hyperledger Composer, scalability concerns, and ensuring compatibility with existing forensic tools.

[6] Digital Evidence Management Model Based on Hyperledger Fabric:

This model outlines a method for creating a secure digital evidence management system using a permissioned blockchain network, Hyperledger Fabric. It involves storing evidence with timestamps and cryptographic identifiers, using smart contracts to automate evidence management tasks, ensuring transparency, and controlling access based on designated roles. Advantages include improved security, immutability, and efficient evidence management. However, drawbacks may involve the need for expertise in blockchain technology and Hyperledger Fabric, along with the costs of implementation and maintenance.

[7] Integrated Model for Digital Forensic Processes:

This study proposes a unified model that consolidates various digital forensic processes by analyzing existing standards and technologies to identify common elements across different forensic stages. The model aims to improve collaboration and efficiency among forensic practitioners by reducing redundancy and facilitating information sharing. While the integrated framework can enhance the effectiveness of forensic investigations, it may face challenges such as the need for community-wide acceptance and the ability to adapt to rapidly evolving forensic technologies.

III. METHODOLOGY OF PROPOSED SURVEY

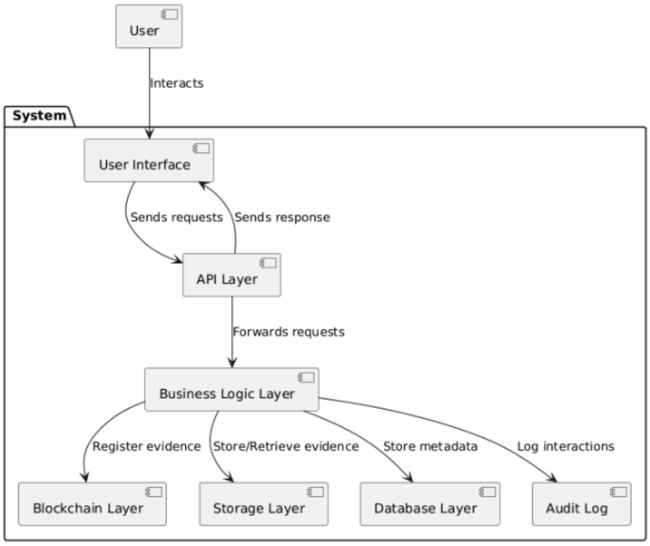
A. REQUIREMENT ANALYSIS

Proposed system must meet following requirement analysis –

System be must designed to meet the needs of law enforcement, legal teams, and forensic experts through various functional requirements. It allows secure uploading of digital evidence documents, images, and videos while restricting access to authorized personnel via a user-friendly interface. Each piece of evidence is registered on the blockchain with timestamps to ensure tamper-proof records, and cryptographic hashes are generated upon upload to verify data integrity. Smart contracts are used to manage access control automatically, and an non tamperable chain of custody record will log all interactions with the evidence. The system will generate detailed audit trails and reports, allowing secure sharing of evidence among authorized users, along with real-time alerts for unauthorized access attempts.On the non-functional side, the system must be scalable to handle increasing volumes of digital evidence, with strong encryption protocols to protect sensitive data. Fast response times for uploading and viewing evidence are essential, along with an friendly user interface that requires minimal training. Compliance with legal regulations, such as GDPR and HIPAA, is necessary, as is ensuring high availability with minimal downtime. Finally, the system must maintain an non tamperable audit trail for all interactions with evidence, facilitating thorough reviews during legal proceedings.Keeping this requirements our proposed system will be developed.

B. SYSTEM ARCHITECTURE

The system architecture consists of several key components, each serving a vital role in the overall functionality of the evidence management system.



User Interface (Frontend) is designed to provide a user-friendly experience for investigators, forensic analysts, and legal teams. Built with React.js, it allows users to securely upload and view digital evidence, including documents, images.

The API Layer (Backend Server) acts as an bridge between the frontend and backend services, handling incoming HTTP/HTTPS requests and routing them to the appropriate services. This layer ensures seamless communication and data flow throughout the system.

The Business Logic Layer consist of the core functionality of the system, managing evidence, user authentication, access control, and interactions with the blockchain and storage services.

The Blockchain Layer employs blockchain platforms to establish tamper-proof records of evidence. This layer is crucial for maintaining the integrity of the data through smart contracts that govern access control, ensuring that only authorized users can interact with the evidence.

In the Storage Layer, AWS cloud stores digital evidences. This layer allows for scalable storage solutions. Local file storage may also be utilized for temporary storage during development.

The Database Layer consists of NoSQL (MongoDB) database. It handle unstructured data, including evidence files and associated metadata.

The Audit & Log Management Layer employs tools like the ELK Stack to facilitate centralized logging and auditing of system activities. This layer captures all interactions with evidence, providing a comprehensive audit trail essential for compliance and legal reviews.

Finally, the Alert System monitors the system for unauthorized access attempts, triggering real-time alerts to system administrators or responsible personnel.

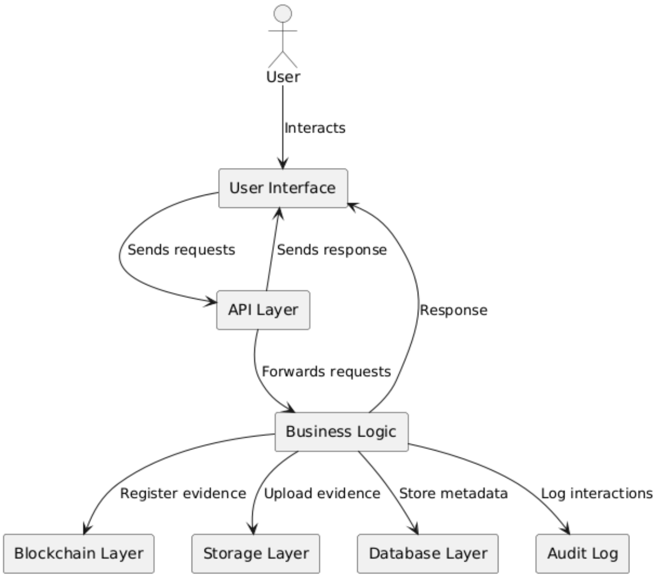


Fig. Data Flow Diagram

Users interact with the User Interface (UI) to perform actions like uploading or viewing evidence. These requests are sent to the API Layer, which forwards them to the Business Logic Layer (BL). The BL processes the requests, managing evidence handling and enforcing access control.

Upon uploading evidence, the BL interacts with the Storage Layer to save evidence files and with the Database Layer to store metadata. Simultaneously, it registers the evidence on the Blockchain Layer, ensuring tamper-proof records for integrity. The Audit Log captures every interaction with the evidence, maintaining an non tamperable record for compliance. Finally, responses are sent back to the UI via the API Layer, providing users with feedback on their actions.

C. TECHNOLOGY STACK

- Frontend
- React.js framework
- Html, Css, Javascript
- Backend

Programming Language: Node.js with Express.js for building RESTful APIs.
-Blockchain Platform for implementing blockchain functionalities.

- Database

NoSQL: MongoDB for storing unstructured data (evidence files, metadata).

- File Storage

Cloud Storage: AWS cloud Storage for securely storing digital evidence.
Local Storage: Use a secure file system for local storage during development or in case of offline access.

- Security

Authentication: JSON Web Tokens (JWT) for secure user authentication and session management.
Encryption: AES and RSA for encrypting sensitive data during transmission and storage.

- Tools and software
- Github : Source code management
- Visual Studio : Development
- ELK stack : logging and monitoring
-

IV. CONCLUSION AND FUTURE WORK

The research and development of the evidence management system underline the importance of leveraging advanced technologies such as blockchain and cloud computing to improve the management of digital evidence. By ensuring data integrity, accountability, and security, the system addresses critical challenges faced by law enforcement and legal professionals in handling sensitive evidence.The positive outcomes observed during user testing shows that the system not only meets functional requirements but also the non-functional requirements such as scalability, performance, and compliance with data privacy regulations. The successful integration of various components ranging from user interface design to backend blockchain operations illustrates a comprehensive approach to modernizing evidence management. Future work will involve refining the system based on user feedback, expanding its functionalities, and conducting larger-scale deployments to evaluate its effectiveness in diverse operational environments. Also leveraging AI in Analysis of evidences is considered in future work. This project sets a strong foundation for ongoing innovation in evidence management, ultimately contributing to more reliable and secure practices in the legal and law enforcement sectors.

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

INTERNATIONAL JOURNAL
OF MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

☎ +91 99405 72462 +91 63819 07438 ✉ ijmrsetm@gmail.com

www.ijmrsetm.com