IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 3, May-June 2025

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203034

Evidence Protection and Assisting Police using Blockchain

Randive Prem[1], Javanjale Mangesh[2], Narnavale Abhishek[3], Prof. Ganesh Avhad[4]

Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar, India[123]

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

ABSTRACT: The growing dependence on digital evidence in law enforcement and legal proceedings highlights the necessity for secure, efficient, and tamper-resistant evidence management systems. This project introduces a blockchain based solution designed to enhance the integrity, traceability, and security of digital evidence. By leveraging blockchain technology, the system establishes a decentralized, immutable ledger that records evidence submissions, access logs, and chain-of-custody details, thereby ensuring transparency and authenticity. This proposed method overcomes the shortcomings of traditional evidence handling practices, which often involve risks of tampering, inefficient manual processes, and inconsistent documentation. With this innovative system, law enforcement agencies can significantly enhance the accuracy and reliability of digital investigations, ultimately building trust and confidence in the judicial process.

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

I. INTRODUCTION

In contemporary law enforcement and judicial systems, maintaining the integrity, security, and traceability of digitalevidence is essential for upholding justice. The surge in digital data utilized in criminal investigations has exposedsignificant shortcomings in traditional evidence management methods, which typically depend on physical storage andmanual processes that are vulnerable to tampering, loss, and unauthorized access. These weaknesses can undermine thecredibility of evidence and potentially influence the outcomes of legal cases. To tackle these issues, this project introduces ablockchain-based evidence management system aimed at transforming the management of digital evidence. Blockchaintechnology provides a decentralized, tamper-resistant ledger that meticulously records evidence transactions with time-stamped logs, thereby ensuring data integrity and transparency. By incorporating blockchain, the proposed systemestablishes a dependable chain of custody and audit trails that can be relied upon in court. Furthermore, the system utilizesscalable cloud storage options for effective evidence management and incorporates smart contracts to automate accesscontrol, ensuring that only authorized personnel can view or modify evidence. This proposed solution mitigates the riskslinked to conventional evidence management while embracing digital technology advancements to improve lawenforcement practices. By adopting this strategy, the project seeks to create a secure, transparent, and efficient frameworkfor managing digital evidence, ultimately enhancing crime-solving capabilities and boosting public trust in the judicialsystem.

II. LITERATURE REVIEW

Implementation of Blockchain Technology in Forensic Evidence Management- Gupta et al., 2021, IEEE: Implementing blockchain technology in the management of forensic evidence entails establishing a secure, decentralized framework forthe storage of digital evidence. This process starts with a distributed ledger that assigns unique cryptographic identifiers toeach piece of evidence, which are logged as transactions. The ledger is upheld by a network of nodes, ensuring that nosingle entity has control over it. Smart contracts can facilitate the automation of evidence verification, thereby enhancingboth reliability and efficiency.

· IoT Forensics System Based on Blockchain- Zawoad &amp; Hasan, 2020, IEEE Xplore: Combining IoT devices with blockchain technology for digital forensics involves collecting and timestamping evidence from IoT sources, which issecurely stored in an immutable blockchain ledger. This decentralized approach ensures data integrity and uses smartcontracts to automate evidence verification, enhancing the security and transparency of forensic investigations. However, challenges such as scalability, implementation costs, and the need for training forensic professionals in blockchain usage may occur.

· Digital Evidence Management Model Based on Hyperledger Fabric Rahman &amp; Hossain, 2022, IEEE : The model outlinesa strategy for creating a secure digital evidence management system using a permissioned blockchain network, specificallyHyperledger Fabric. It involves storing evidence with timestamps and cryptographic identifiers, using smart contracts forautomation, ensuring transparency, and controlling access based on roles. Benefits include improved security, immutability,and efficient evidence management. However, challenges include the need for specialized blockchain knowledge andpotential costs for implementation and maintenance.

· Secure Evidence Management in Digital Forensics Using Blockchain- Lee &amp; Kim, 2022, Springer : Blockchain provides adecentralized and secure method for managing digital evidence in forensics by creating a tamperproof ledger thattimestamps and authenticates each piece of evidence with cryptographic identifiers. This enhances integrity and trustthrough consensus mechanisms that prevent unauthorized changes. However, challenges such as scalability and compliancewith legal standards for court admissibility remain.

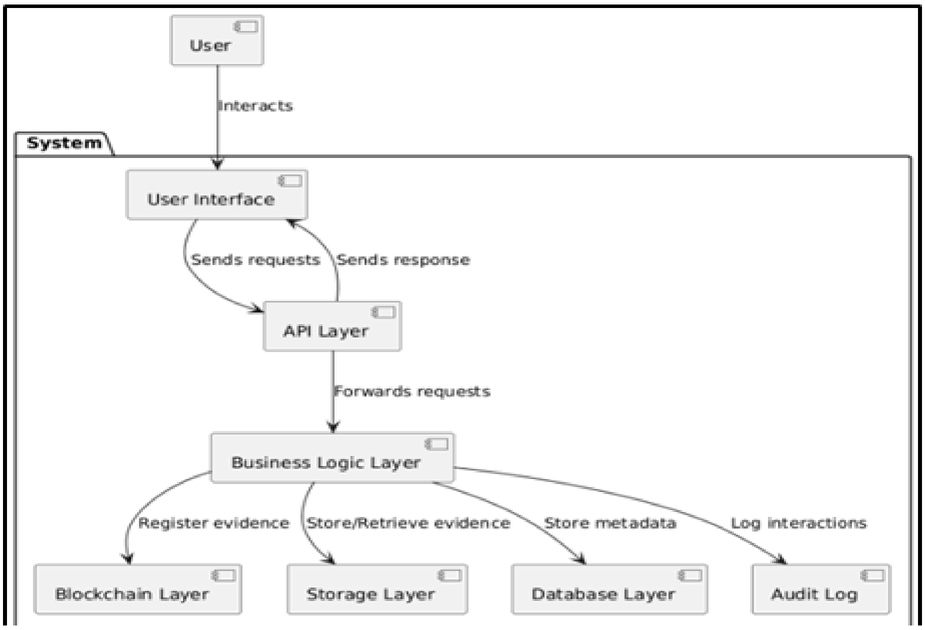
· Forensic-Chain: Blockchain-Based Digital Forensics Chain of Custody Using Hyperledger Composer- Alam et al., 2021,IEEE. The Forensic-Chain framework establishes a decentralized and immutable ledger for managing the digital forensicschain of custody, demonstrated through a Proof of Concept using Hyperledger Composer. Each forensic item receives aunique identifier, and all transactions are recorded on the blockchain, ensuring a tamper-proof and auditable custody trail.This approach enhances security and transparency by utilizing blockchain&#39;s decentralized nature and Hyperledger Composer&#39;s custom functionalities.

III. PROBLEM STATEMENT

The management of evidence in legal and law enforcement faces significant challenges, including tampering, inefficienttracking, limited accessibility, and data privacy concerns. Traditional evidence management systems often rely on paperrecords, which are prone to human error, leading to compromised integrity and difficulties in maintaining a secure chain ofcustody. Additionally, sensitive information related to evidence may be mishandled or exposed, raising ethical and legalissues. Digital Provenance:

IV. SYSTEM ARCHITECTURE

The system architecture consists of several key components, each serving a vital role in the overall functionality of theevidence management system a. ARCHITECTURE The system architecture is made up of several essential User Interface(Frontend) is designed to provide a user-friendly experience for investigators, forensic analysts, and legal teams. Built withReact.js, it allows users to securely upload and view digital evidence, including documents, images, and videos.



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 dataflow throughout the system.

The Business Logic Layer consist of the core functionality of the system, managing evidence, user authentication, accesscontrol, 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 formaintaining 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 &amp; 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.

V. 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 dataintegrity, accountability, and security, the system addresses critical challenges faced by law enforcement and legalprofessionals in handling sensitive evidence. The positive outcomes observed during user testing shows that the system notonly meets functional requirements but also the non-functional requirements such as scalability, performance, andcompliance with data privacy regulations. The successful integration of various components ranging from user interfacedesign to backend blockchain operations illustrates a comprehensive approach to modernizing evidence management. will involve refining the system based on user feedback, expanding its functionalities, and conducting larger-scaledeployments to evaluate its effectiveness in diverse operational environments. Also leveraging AI in Analysis of evidencesis 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.

DOI:10.15680/IJARETY.2025.1203034

REFERENCES

1) Yan wu , Fang Lu Lu , “A Bitcoin Transaction Network Analysis Method for Future Blockchain ForensicInvestigation”-2023

2) M. Sharma et al., “LoED: LoRa and edge computing based system architecture for sustainable forestmonitoring,” 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 inmonitoring 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 cloudcomputing,” 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 blockchaintechnology 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 ThirdInternational 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

IJARETY

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com