IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 10, October 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

© 2024 IJIRCCE | Volume 12, Issue 10, October 2024| DOI: 10.15680/IJIRCCE.2024.1210069

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Evidence Protection and Assisting Police Using Blockchain

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

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

Professor, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, Ahmednagar, Maharashtra, 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 digital evidence is essential for upholding justice. The surge in digital data utilized in criminal investigations has exposed significant shortcomings in traditional evidence management methods, which typically depend on physical storage and manual processes that are vulnerable to tampering, loss, and unauthorized access. These weaknesses can undermine the credibility of evidence and potentially influence the outcomes of legal cases. To tackle these issues, this project introduces a blockchain-based evidence management system aimed at transforming the management of digital evidence.

Blockchain technology 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 system establishes a dependable chain of custody and audit trails that can be relied upon in court. Furthermore, the system utilizes scalable cloud storage options for effective evidence management and incorporates smart contracts to automate access control, ensuring that only authorized personnel can view or modify evidence.

This proposed solution mitigates the risks linked to conventional evidence management while embracing digital technology advancements to improve law enforcement practices. By adopting this strategy, the project seeks to create a secure, transparent, and efficient framework for managing digital evidence, ultimately enhancing crime-solving capabilities and boosting public trust in the judicial system.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE SURVEY

- **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 for the storage of digital evidence. This process starts with a distributed ledger that assigns unique cryptographic identifiers to each piece of evidence, which are logged as transactions. The ledger is upheld by a network of nodes, ensuring that no single entity has control over it. Smart contracts can facilitate the automation of evidence verification, thereby enhancing both reliability and efficiency.

- **IoT Forensics System Based on Blockchain- Zawoad & Hasan, 2020, IEEE Xplore:**

Combining IoT devices with blockchain technology for digital forensics involves collecting and timestamping evidence from IoT sources, which is securely stored in an immutable blockchain ledger. This decentralized approach ensures data integrity and uses smart contracts 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 & Hossain, 2022, IEEE :**

The model outlines a strategy for creating a secure digital evidence management system using a permissioned blockchain network, specifically Hyperledger Fabric. It involves storing evidence with timestamps and cryptographic identifiers, using smart contracts for automation, 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 and potential costs for implementation and maintenance.

- **Secure Evidence Management in Digital Forensics Using Blockchain- Lee & Kim, 2022, Springer :**

Blockchain provides a decentralized and secure method for managing digital evidence in forensics by creating a tamper-proof ledger that timestamps and authenticates each piece of evidence with cryptographic identifiers. This enhances integrity and trust through consensus mechanisms that prevent unauthorized changes. However, challenges such as scalability and compliance with 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 forensics chain of custody, demonstrated through a Proof of Concept using Hyperledger Composer. Each forensic item receives a unique 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's decentralized nature and Hyperledger Composer's custom functionalities.

III. PROBLEM STATEMENT

The management of evidence in legal and law enforcement faces significant challenges, including tampering, inefficient tracking, limited accessibility, and data privacy concerns. Traditional evidence management systems often rely on paper records, which are prone to human error, leading to compromised integrity and difficulties in maintaining a secure chain of custody. Additionally, sensitive information related to evidence may be mishandled or exposed, raising ethical and legal issues.

IV. PROPOSED SYSTEM

By utilizing blockchain technology, this system guarantees that all evidence records are stored in an immutable, decentralized ledger, which prevents tampering and enhances transparency. It also integrates smart contracts to automate access control, ensuring that only authorized personnel can view or modify the evidence. Furthermore, scalable cloud storage is implemented to efficiently handle large volumes of data, providing secure and reliable access.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

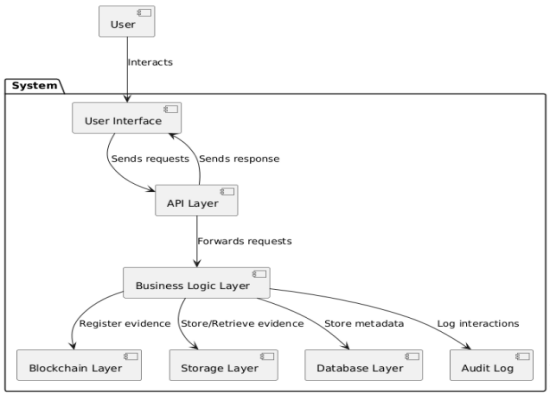

Fig.1: Proposed System Architecture

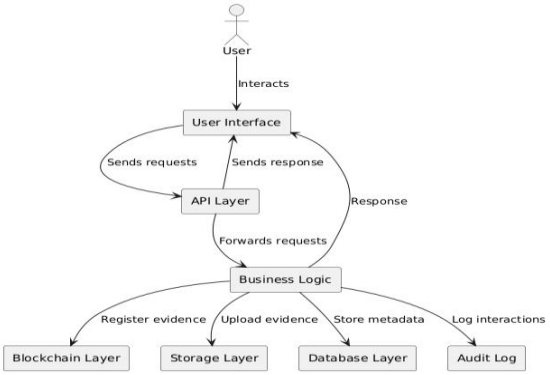

Fig.2: Data Flow Diagram

a. **ARCHITECTURE**

The system architecture is made up of several essential components, each playing a crucial role in the overall operation of the evidence management system.

- **The User Interface** (Frontend) is crafted to deliver an intuitive experience for investigators, forensic analysts, and legal teams.
- **The API Layer** (Backend Server) serves as a conduit between the frontend and backend services, managing incoming HTTP/HTTPS requests and directing them to the appropriate services.
- **The Business Logic Layer** encompasses the system's core functionalities, overseeing evidence management, user authentication, access control, and interactions with blockchain and storage services.
- **The Blockchain Layer** utilizes blockchain technology to create tamper-proof records of evidence.
- In **the Storage Layer**, AWS cloud serves as a repository for digital evidence, offering scalable storage solutions. Additionally, local file storage can be used for temporary storage during the development phase.
- **The Database Layer** is powered by a NoSQL database (MongoDB) that manages unstructured data, including evidence files and their associated metadata.
- **The Audit & Log Management Layer** utilizes tools such as the ELK Stack to enable centralized logging and auditing of system activities.
- Lastly, the Alert System continuously monitors for unauthorized access attempts, generating real-time alerts for system administrators or designated personnel.

b. DATAFLOW

- Users engage with the User Interface (UI) to carry out tasks such as uploading or viewing evidence. These actions are communicated to the API Layer, which relays them to the Business Logic Layer (BL). The BL processes these requests, overseeing evidence management and enforcing access controls.
- When evidence is uploaded, the BL collaborates with the Storage Layer to save the evidence files and with the Database Layer to record metadata. At the same time, it registers the evidence on the Blockchain Layer, ensuring that the records are tamper-proof for integrity.
- The Audit Log tracks every interaction with the evidence, creating a non-tamperable record for compliance purposes. Finally, responses are returned to the UI through the API Layer, offering users feedback on their actions.

TECHNOLOGY STACK

Frontend:

Framework: React.js
Technologies: HTML, CSS, JavaScript

Backend:

Programming Language: Node.js with Express.js for creating RESTful APIs.
Blockchain Platform: Utilized for integrating blockchain functionalities.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Database:
NoSQL: MongoDB for managing unstructured data, such as evidence files and metadata.

File Storage:
Cloud Storage: AWS Cloud Storage
Local Storage.

Security:
Authentication: JSON Web Tokens (JWT).
Encryption: AES and RSA

Tools and Software:
GitHub: Source code management
Visual Studio: Development environment
ELK Stack: For logging and monitoring purposes.

V. CONCLUSION

The development of this evidence management system highlights the significance of utilizing cutting-edge technologies like blockchain and cloud computing to enhance the handling of digital evidence. By prioritizing data integrity, accountability, and security, the system effectively tackles key challenges encountered by law enforcement and legal professionals in managing sensitive information.

The favorable results from user testing indicate that the system fulfills not only its functional requirements but also essential non-functional aspects, including scalability, performance, and adherence to data privacy regulations. The effective integration of diverse components, from user interface design to backend blockchain processes, demonstrates a holistic strategy for modernizing evidence management.

The future development of the blockchain-based evidence management system aims to enhance the platform by incorporating user feedback, broadening its features, and integrating AI for sophisticated evidence analysis. Ongoing user engagement will create feedback loops that facilitate iterative design enhancements, improving both usability and efficiency. The expansion of functionalities will encompass advanced evidence tracking, compatibility with current law enforcement systems, and support for multiple languages to serve a wider range of users. Pilot programs will be conducted in diverse operational settings to assess adaptability and performance, with the potential shift to cloud-based solutions for better scalability.

ACKNOWLEDGMENT

We would prefer to give thanks the researchers likewise publishers for creating their resources available. We are conjointly grateful to guide, reviewer for their valuable suggestions and also thank the college authorities for providing the required infrastructure and support.

REFERENCES

1. Yan wu , Fang Lu Lu , “A Bitcoin Transaction Network Analysis Method for Future Blockchain Forensic Investigation”-2023
2. Robust and secure evidence management in digital forensics investigations using blockchain technology 2023.
3. 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
4. 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
5. E. E.-D. Hemdan and D. H. Manjaiah, “An efficient digital forensic model for cybercrimes investigation in cloud computing,” Multimed. Tools Appl., 2021.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

6. Y. Maleh, and L. Tawalbeh, Artificial intelligence and blockchain for future cybersecurity applications, vol. 90. Springer Nature, 2021.
7. R. Sathyaprakasan, P. Govindan, S. Alvi, L. Sadath, S. Philip, and N. Singh, "An implementation of blockchain technology in forensic evidence management," in 2021
8. International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021
9. 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
10. Y. Baddi, M. Alazab "Forensic Evidence Security System using Blockchain Technology."- 2021
11. R. Singh et al., "Cloud server and Internet of Things assisted system for stress monitoring, Electronics (Basel), vol. 10, no. 24, p. 3133, 2021
12. H. Lone and R. N. Mir, "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer," Digit. Investig., vol. 28, pp. 44–55, 2019

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details