ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

BLOCKCHAIN DRIVEN EVIDENCE MANAGEMENT SYSTEM

[1] Tasneem Rahath, [2] V.Manaswini,[3] S.Manisha,[4] N.Pavani

[1]Assistnat Professor in Department of Information Technology, Bhoj Reddy Engineering College for Women

[2,3,4,]UG Scholars in Department of Information Technology, Bhoj Reddy Engineering College for Women

Abstract

The traditional e-FIR (First Information Report) system suffers from multiple critical vulnerabilities due to its centralized design, including the risks of data tampering, unauthorized access, and manipulation of records. These issues undermine public trust and enable the misuse of the complaint registration system, often leading to false allegations and administrative corruption. This paper proposes a blockchain-based decentralized e-FIR system designed to address these challenges by ensuring secure, immutable, and transparent handling of FIR records. The proposed framework eliminates reliance on intermediaries, enhances data integrity through distributed ledger technology, and supports tamper-proof storage of complaints and evidence. By improving the traceability, accountability, and accessibility of records, the system aims to restore public confidence and strengthen the reliability of law enforcement processes.

I INTRODUCTION

The digitization of law enforcement services has improved accessibility and efficiency, particularly through systems like e-FIR portals that allow citizens to report crimes online. However, these centralized systems are increasingly exposed to a range of vulnerabilities that compromise their effectiveness and credibility. Data tampering, hacking, and the submission of fake complaints are major concerns that not only delay justice but also erode public trust in the criminal justice system. Furthermore, the involvement of intermediaries often introduces risks of corruption and operational inefficiencies. To overcome these limitations, there is an urgent need for a decentralized and secure framework that ensures the authenticity, integrity, and traceability of registered complaints and related data. Blockchain technology, with its immutable ledger and distributed consensus mechanisms, offers a promising solution. This paper introduces a blockchain-powered e-FIR system that not only safeguards complaint data from manipulation but also simplifies the verification process, reduces administrative burden, and enhances user trust through transparent record-keeping. The proposed system aims to modernize the complaint registration process and reinforce the foundational principles of accountability and justice in law enforcement.

II LITERATURE SURVEY

The evolution of complaint handling and evidence management systems has seen a growing interest in blockchain technology due to its ability to enhance security, transparency, and trust. Numerous studies have explored its potential in transforming centralized and vulnerable systems into robust, tamper-proof architectures.

Gupta et al. (2019) introduced a blockchain-based FIR system that effectively eliminates intermediaries, emphasizing decentralization and immutability as critical components for enhancing trust and reliability in law enforcement processes [1]. Similarly, Tabassum et al. (2018) underscored the need for user-friendly platforms that allow citizens to file complaints remotely, thus improving both accessibility and system efficiency [2].

Onuiri et al. (2015) developed a real-time crime records management system, demonstrating that structured digital record-keeping can significantly improve decision-making and contribute to crime reduction [3]. Building on this, Kim et al. (2021) proposed a two-level blockchain architecture for digital evidence management, ensuring data integrity and availability through decentralized mechanisms [4].

Hingorani et al. (2020) highlighted the importance of automated updates within such systems to bridge communication gaps between law enforcement agencies and the public, thereby fostering greater public trust [5]. Dini et al. (2018) further explored the role of blockchain in criminal record systems, focusing on secure and agile information sharing among various stakeholders [6].

Mollah et al. (2012) presented an integrated e-policing solution combining biometric verification and traffic management, indicating the broader applications of smart technologies in enhancing police workflows and operational effectiveness [7]. Leible et al. (2019) emphasized the need for open, decentralized systems to prevent single points of failure and promote transparent data handling [8].

Security enhancements through cryptographic mechanisms and smart contracts were explored by Rao et al. (2020), who demonstrated blockchain's utility in securing data against tampering and unauthorized access [9]. Makalew (2022) focused on the user experience aspect, proposing role-based access control and intuitive interfaces as key to improving usability and security simultaneously [10]. Finally, Garcia and Claour (2021) examined decentralized storage solutions such as IPFS, highlighting their effectiveness in improving scalability and reducing reliance on centralized servers [11].

Collectively, these studies validate the growing consensus that blockchain technology offers a transformative approach to modernizing e-FIR systems, ensuring enhanced data security, integrity, and public trust.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

III EXISTING SYSTEM

The current evidence management systems deployed in legal, forensic, and investigative environments primarily operate through centralized databases or manual record-keeping. These traditional systems are increasingly proving to be inadequate in safeguarding the integrity, confidentiality, and authenticity of digital or physical evidence. Centralized systems inherently possess single points of failure, which make them vulnerable to data breaches, tampering, and unauthorized alterations.

In legal contexts, the credibility of evidence is paramount. However, existing systems fall short in guaranteeing that evidence remains unaltered from the point of collection to its presentation in court. Manual documentation of the **chain of custody** often lacks efficiency, is prone to human errors, and does not support real-time verification. Moreover, there is limited transparency in how complaints or evidence are handled, which reduces trust among the involved stakeholders such as law enforcement agencies, legal teams, and citizens.

Disadvantages of the Existing System:

Data Tampering: Centralized architecture allows a single point of control, increasing the risk of intentional or accidental data manipulation.

Lack of Transparency: There is no clear audit trail or transparent record for tracking the lifecycle of evidence or complaints.

Unauthorized Access: Weak access control mechanisms can lead to data breaches, exposing sensitive information.

Manual and Inefficient Processes: Dependency on manual procedures for logging, verifying, and transferring evidence leads to inefficiencies and delays.

Limited Trust: Due to these vulnerabilities, users often question the reliability and impartiality of the evidence management process.

IV PROBLEM STATEMENT

The existing e-FIR (First Information Report) system is hindered by its centralized framework, which exposes it to multiple security and operational vulnerabilities. This architecture increases the risk of data tampering, where unauthorized changes can compromise the integrity and authenticity of recorded information. Additionally, the system is prone to cyberattacks, endangering the confidentiality and availability of critical data. The lack of robust verification mechanisms also permits the submission of false complaints, contributing to system abuse and a decline in public trust. Furthermore, reliance on intermediaries fosters opportunities for corruption and administrative inefficiencies, weakening the effectiveness of crime tracking and law enforcement processes. These limitations underscore the urgent need for a more secure, transparent, and decentralized solution for

managing complaints and sensitive records in the policing ecosystem.

V OBJECTIVE

The proposed system aims to address these challenges by introducing a blockchain-based framework that ensures enhanced security, data integrity, and traceability. The key objectives include implementing tamper-proof data storage, minimizing the incidence of fraudulent complaint registrations, and improving transparency and accessibility. By leveraging decentralization and cryptographic safeguards, the system seeks to streamline the complaint management process, foster accountability, and restore public confidence in law enforcement and justice delivery mechanisms.

VI PROPOSED SYSTEM

The proposed system introduces a **blockchain-enabled e-Police System (EPS)** designed to overcome the limitations of existing centralized e-FIR platforms. By utilizing blockchain technology, the system ensures secure, transparent, and tamper-resistant handling of complaint records and evidence.

At its core, the system employs a **decentralized and distributed blockchain ledger** to record and manage FIR data and supporting evidence. Each piece of information is cryptographically hashed and timestamped, creating an immutable digital footprint that prevents unauthorized modifications. This ensures the authenticity and integrity of data throughout its lifecycle.

The use of **smart contracts** enables automated validation and access control, enforcing role-based permissions for law enforcement officers, judiciary members, and authorized stakeholders. In addition, the system supports real-time updates and traceability, allowing for seamless auditability and enhanced user trust.

By eliminating the dependency on centralized servers and intermediaries, the proposed EPS mitigates the risk of single points of failure, corruption, and data manipulation—making it a robust and reliable solution for modern law enforcement needs.

Advantages

Enhanced Data Security and Immutability: Blockchain ensures that once data is recorded, it cannot be altered or deleted, preserving the integrity of FIRs and evidence.

Increased Trust and Transparency: All actions are logged transparently on the distributed ledger, fostering public trust in the law enforcement system.

Elimination of Intermediaries: Direct citizen-to-system interaction reduces bureaucratic layers, minimizing opportunities for corruption and delays.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

Decentralized Access Control: Role-based permissions via smart contracts grant secure, selective access to authorized entities.

Fraud Prevention and Data Privacy: Cryptographic protections and secure identity verification reduce false complaint registrations and unauthorized data exposure.

Scalability and Efficiency: The distributed nature of the system allows it to scale as needed without compromising performance or reliability.

Improved Accessibility: Citizens can lodge complaints remotely and securely, promoting digital inclusion and timely justice delivery.

VII IMPLEMENTATION

The Blockchain-Driven Evidence Management System is designed around five key functional modules, each of which contributes to building a secure, transparent, and decentralized digital evidence handling platform. These modules work in unison to maintain the authenticity, integrity, and traceability of sensitive data and complaint records.

The **Add Information** module is responsible for enabling users—including police personnel, legal authorities, and citizens—to upload various forms of digital evidence such as images, documents, or text files. Once a file is uploaded, the system automatically generates a unique cryptographic hash (typically using SHA-256) to represent the file's content securely. This hash, along with essential metadata such as the timestamp, user ID, and a brief description, is stored immutably on the Ethereum blockchain using smart contracts. To maintain efficiency and scalability, the actual file is stored off-chain using decentralized storage solutions like IPFS (InterPlanetary File System) or secure cloud environments. This architecture ensures tamper-resistance, traceability, and long-term integrity of digital evidence.

The **Check Information** module is used to verify the authenticity and current state of any stored digital evidence. Users can search using parameters such as hash value, user ID, or keyword. Upon retrieval, the system provides the original hash and metadata stored on the blockchain. To validate integrity, the system re-hashes the user-provided file and compares it with the original blockchain-stored hash. A successful match confirms that the evidence remains unaltered since submission, providing verifiable proof and a transparent audit trail—essential features in legal and criminal investigations.

The **Smart Contracts Management** module is integral for automating the logic and rules governing the submission, verification, and access control of digital evidence. Smart contracts execute predefined rules without

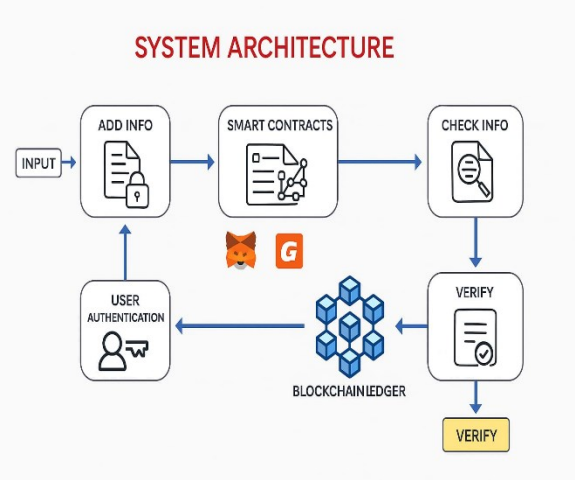
ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

human intervention, ensuring that each action—such as preventing duplicate uploads or blocking unauthorized access—is carried out consistently and securely. These contracts help streamline operations by minimizing manual oversight and potential human error

The **User Authentication** module ensures that only verified and authorized users can interact with the system. This is achieved through decentralized identity verification mechanisms, often involving Ethereum-compatible wallets such as MetaMask. Every user action, whether adding or checking information, is linked to a blockchain address, thereby ensuring accountability and traceability. This decentralized login mechanism not only enhances system security but also reduces reliance on traditional, centralized credential systems that are more susceptible to breaches.

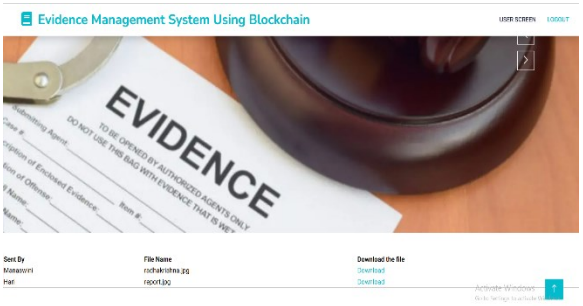
Finally, the **Blockchain Ledger Interface** serves as the communication layer between the application and the Ethereum blockchain. It utilizes tools like Web3.js or Web3.py to manage all blockchain transactions and data retrieval operations. This module abstracts the complexity of the underlying blockchain operations, handling tasks such as sending transactions, confirming their execution, and reading smart contract logs. It also fetches historical records including hashes and timestamps to support verification and audits. By replacing the need for a centralized backend database, this module ensures data integrity, consistency, and decentralization throughout the system.

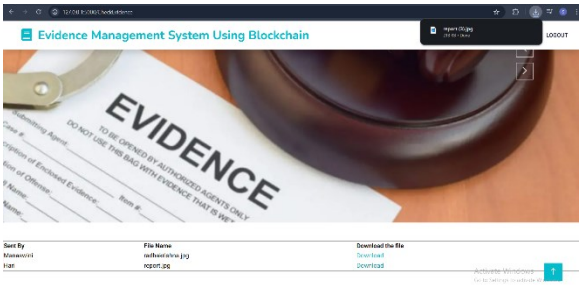
VIII SYSTEM ARCHITECTURE

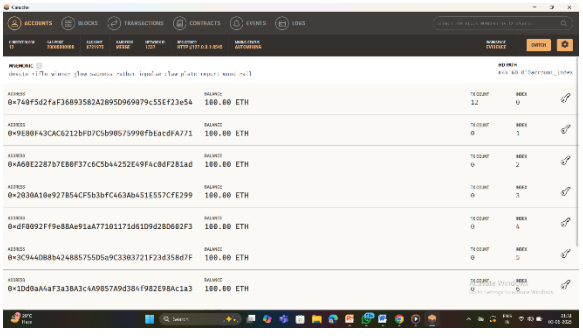


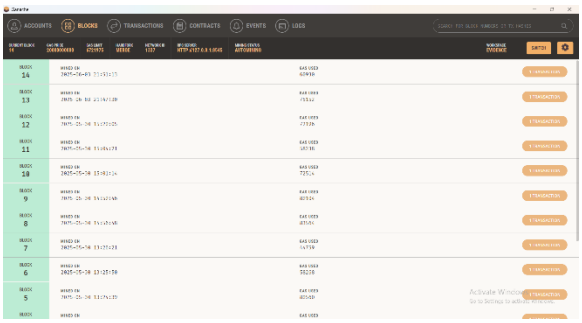
IX RESULTS

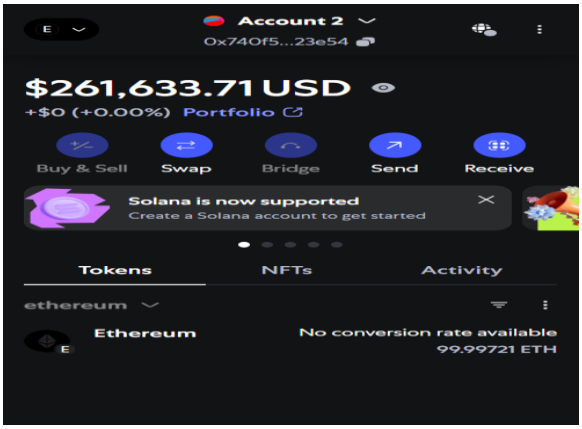
ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025











X CONCLUSION

The blockchain-based evidence protection system represents a transformative approach to digital evidence management. By harnessing the decentralized and transparent nature of blockchain technology, the system ensures the integrity, security, and immutability of evidence. Each piece of evidence is cryptographically secured and time-stamped, creating a tamper-proof audit trail that significantly enhances the reliability and trustworthiness of the data.

This system not only protects evidence from unauthorized access and alterations but also

facilitates secure verification by authorized users through transparent yet controlled access mechanisms. The reduction in human intervention and reliance on automated smart contracts improves operational efficiency and minimizes the risk of errors or manipulation.

Overall, the proposed solution offers a scalable, secure, and trustworthy framework for evidence management, making it highly suitable for law enforcement, legal, financial, and other sensitive domains. Its potential to reduce corruption, enhance accountability, and build public trust positions it as a vital tool for modern digital governance and compliance infrastructures.

REFERENCES

[1] Sumit Kumar Rana, Arun Kumar Rana, Sanjeev Kumar Rana, Vishnu Sharma, Umesh Kumar Lilhore, Osamah Ibrahim Khalaf, Antonino Galletta, "Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain", IEEE Access, vol.11, pp.83289-83300, 2023.

[2] Z. Tian, M. Li, M. Qiu, Y. Sun and S. Su, "Block-DEF: A secure digital evidence framework using blockchain", Inf. Sci., vol. 491, pp. 151-165, Jul. 2019.

[3] Hu Liu, Yuxuan Liu, "Construction of a Medical Resource Sharing Mechanism Based on Blockchain Technology: Evidence from the Medical Resource Imbalance of China" published in Healthcare 1 January 2021, DOI:10.3390/healthcare9010052

[4] M. H. Mollah, M. A. K. Azad, A. Vasilakos, "Security and Privacy Challenges in Mobile Cloud Computing: Survey and Way Ahead," *Journal of Network and Computer Applications*, vol. 84, pp. 38–54, Apr. 2017.

[5] F. Casino, T. K. Dasaklis, and C. Patsakis, "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues," *Telematics and Informatics*, vol. 36, pp. 55–81, Mar. 2019.

[6] Q. Wang, Y. Zhu, J. Xu, and Z. Li, "Security and Privacy of Blockchain: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 258–312, 1st Quart., 2021.

[7] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," *arXiv preprint*

arXiv:1608.05187, 2016.

[8] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, vol. 2, pp. 6–10, Jun. 2016.

[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, 2008. 2019.

[Online]. Available: https://bitcoin.org/bitcoin.pdf

[10] X. Zheng, S. Yang, W. Wu, M. Guo, and C. E. Palazzi, "Smart Contract-Based Access Control for the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, Apr.