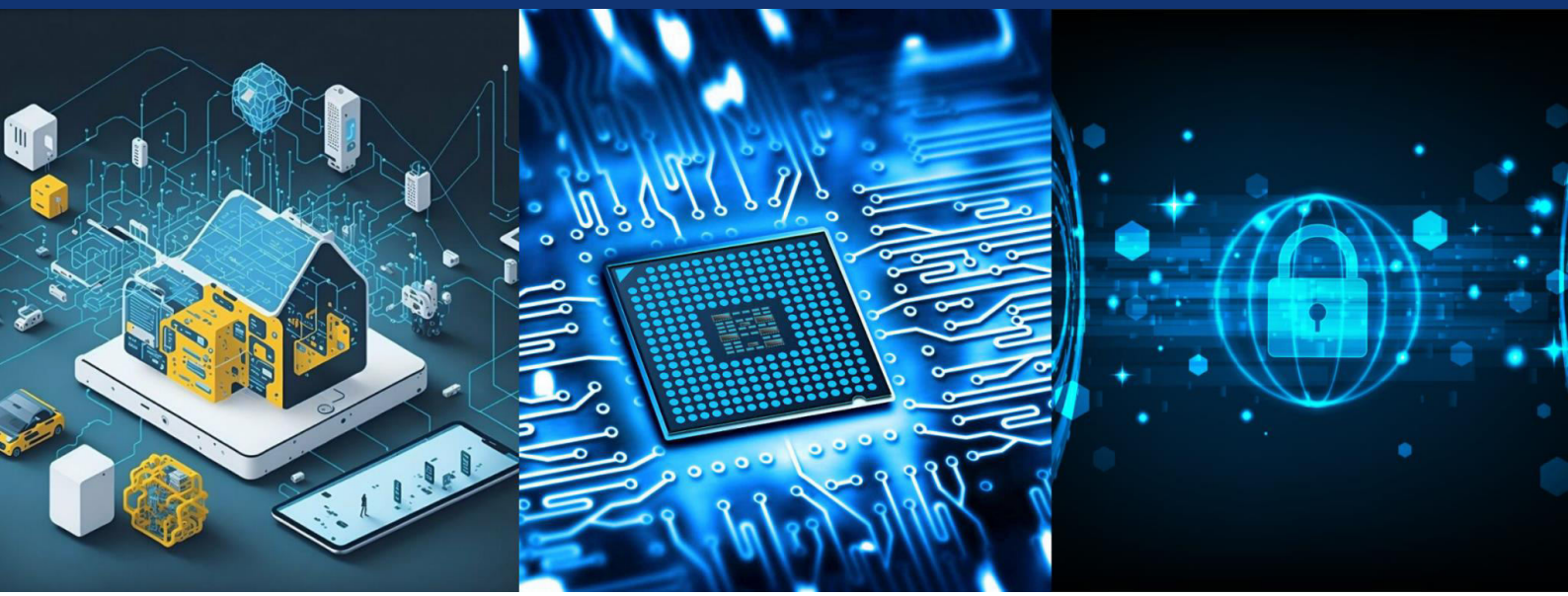
IJIRCCE

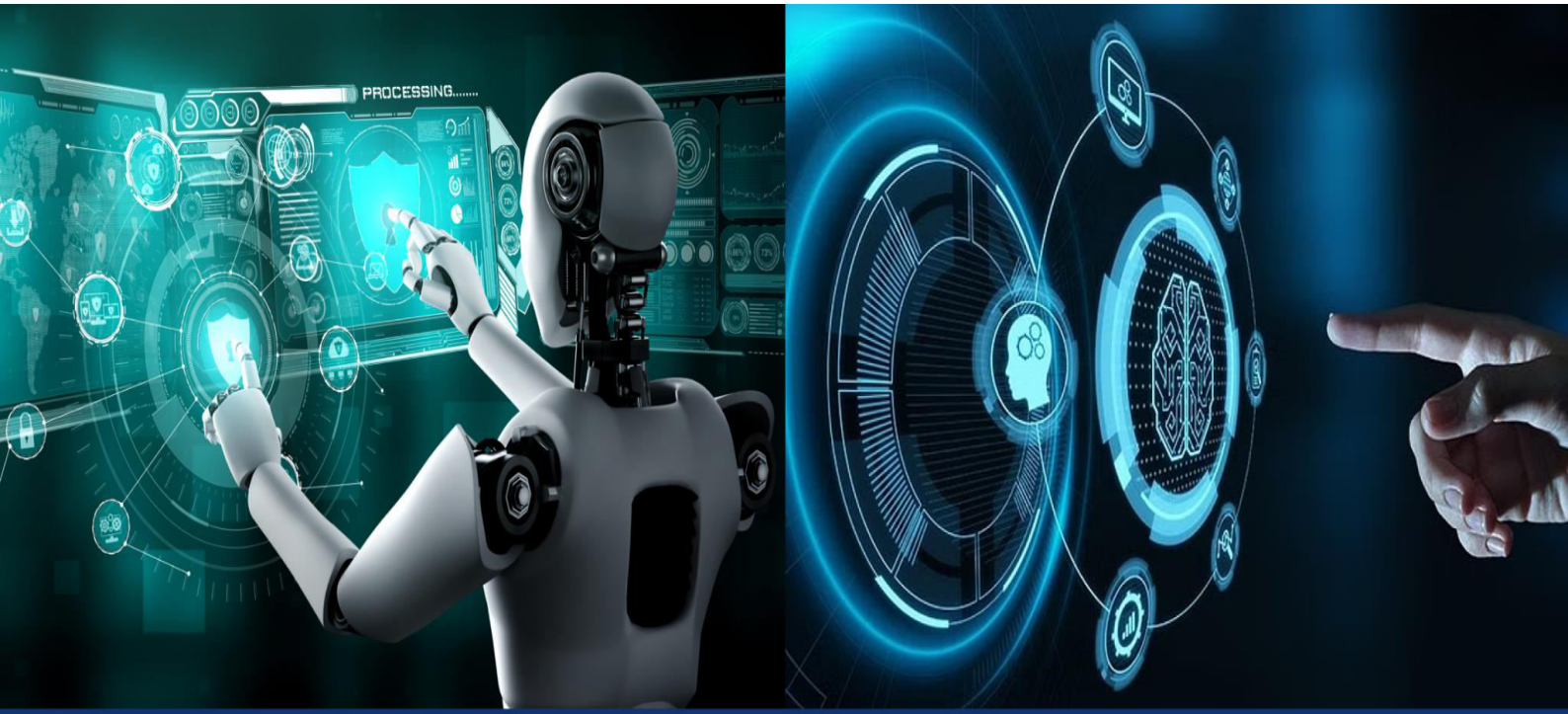
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

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



Impact Factor: 9.927

Volume 14, Issue 5, May 2026

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405008

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

Blockchain based Tamper-proof System for FIR and Evidence Integrity

Swamiraj Jadhav, Devansh Patil, Viraj Patil, Tanishq Nikam, Vaibhavi Nawale

Department of Computer Engineering, AISSMS College of Engineering, Savitribai Phule Pune University, Pune, India

ABSTRACT: The conventional First Information Report (FIR) framework faces several persistent challenges, including vulnerability to data manipulation, limited transparency, procedural delays, and weak protection of digital evidence. These limitations can undermine public confidence in law enforcement systems. To overcome these issues, this study proposes a Blockchain-Based FIR and Evidence Integrity System designed to ensure secure, transparent, and dependable record management.

The proposed solution leverages Ethereum blockchain technology to record FIR data in a way that prevents unauthorized modification. Once information is stored, it becomes permanently verifiable. Automated workflows are implemented through smart contracts, enabling efficient FIR registration, validation, and status tracking without manual intervention. Since blockchain storage is not suitable for large multimedia files, the system integrates IPFS (InterPlanetary File System), where evidence files are stored externally while their corresponding content identifiers (CIDs) are recorded on-chain. This mechanism ensures that any alteration in the stored file can be easily identified through hash discrepancies.

Additionally, the system incorporates a responsive user interface developed using React.js, supported by a Node.js backend, along with secure authentication protocols to regulate access and user roles.

Experimental outcomes indicate that the system successfully safeguards records against unauthorized modifications, provides a transparent history of all transactions, and enables real-time monitoring of FIR progress. Any attempt to alter stored data is immediately flagged due to inconsistencies in hash values.

Overall, this approach offers a robust and scalable enhancement to existing FIR systems by strengthening data integrity, improving accountability, and fostering greater trust between citizens and law enforcement agencies.

KEY WORDS: Blockchain, FIR System, Data Integrity, Smart Contracts, IPFS, Digital Evidence Security.

I. INTRODUCTION

In the Indian criminal justice system, the FIR acts as a basic document that triggers legal action in any case involving a cognizable offense. It is the first interaction between a citizen and law enforcement agencies, which acts as a basis for investigation and prosecution in a case. However, there are a number of disadvantages in traditional FIR management systems, which are either based on a physical system or a centralized digital system.

Some of these disadvantages include data tampering, a lack of transparency, and corruption in the system. As systems become more digital, protecting sensitive data has become very important. Most existing systems are centralized, which makes them vulnerable to unauthorized access, data manipulation, and system failures. Because of this, there is a strong need for a system that ensures data integrity, transparency, and security.

To overcome these disadvantages, this study proposes a new system, referred to as VeriFIR, which is a blockchain-based FIR management system, ensuring a tamper-proof system, decentralized evidence management, and transparent verification mechanisms. The proposed system will increase the level of trust, accountability, and reliability in law enforcement activities.

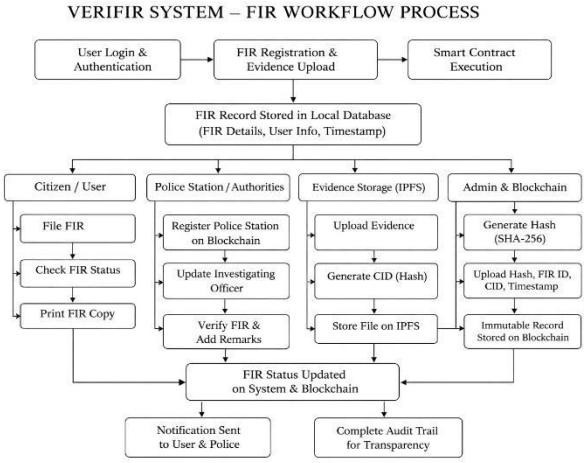
© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405008

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

III. SYSTEM OVERVIEW



The proposed VeriFIR system brings together blockchain technology, distributed storage, and modern web-based interfaces to create a secure, transparent, and tamper-proof platform for FIR management and digital evidence handling. It is designed to support different stakeholders—citizens, police authorities, and administrators—through dedicated functional modules, while ensuring smooth and secure data flow across the entire system.

The process begins with user authentication, where both citizens and police personnel log into the platform using role-based access mechanisms. Once logged in, the citizen panel allows users to register a First Information Report (FIR) by entering the required details and uploading supporting evidence such as images, videos, or documents. The system focuses onsimplicity and usability, while also ensuring proper data validation at the input stage.

When evidence is uploaded, it is handled using IPFS (InterPlanetary File System), a decentralized storage mechanism. Each file generates a unique Content Identifier (CID), which acts as a cryptographic fingerprint. Instead of storing large files directly on the blockchain, only the CID is linked to the FIR. This approach not only improves efficiency but also maintains data integrity, as even a small change in the file results in a different CID, enabling easy tamper detection.

At the same time, FIR data is processed through the backend system, which manages communication between the frontend, database, IPFS, and blockchain network. Key details such as FIR ID, timestamp, and evidence hash (CID) are securely recorded on the blockchain using smart contracts. Once stored, the data becomes immutable, transparent, and verifiable, ensuring that no unauthorized changes can be made.

The police panel enables authorities to manage FIRs effectively. It includes features such as registering police stations, assigning investigating officers, verifying FIR details, and updating case status. All actions performed are recorded within the system, ensuring accountability and traceability.

The admin panel handles system-level responsibilities, including hash generation, blockchain interaction, and maintaining system integrity. It ensures that all records are properly validated before being stored on the blockchain, helping maintain a consistent and reliable system structure.

In addition to blockchain storage, a database layer (MongoDB or Firebase) is used to store non-critical data such as user profiles and FIR metadata. This allows for faster data access and better system performance, creating a balanced approach by combining centralized and decentralized components.

To strengthen security, the system uses SHA-256 hashing for data integrity, encryption for protecting sensitive information, and secure authentication methods to prevent unauthorized access. It also includes a tamper detection mechanism, where any mismatch between stored hashes and current data signals potential manipulation.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

The system further enhances user experience by providing real-time status updates, notifications, and a complete audit trail. Every step—from FIR registration to verification and updates—is recorded, ensuring full transparency and traceability.

Overall, the VeriFIR system presents a practical and modern solution for FIR management by combining role-based access, blockchain immutability, IPFS-based storage, and automated workflows. This integrated approach not only improves efficiency but also builds trust, making the system scalable and suitable for real-world implementation.

IV. METHODOLOGY

Proposed Blockchain-Based FIR and Evidence Integrity Management System (VeriFIR) is developed following a modular and layered architecture that incorporates contemporary web technologies and a blockchain-based framework for ensuring transparency and tamper-resistance of the FIR data and evidence.
The overall system architecture is divided into five major components:

- User Interface Layer
- Backend Application Layer
- Blockchain Layer
- Off-chain Storage Layer
- Database Layer

These components are interconnected via APIs and blockchain-based interactions. The overall architecture is a good blend of performance, scalability, and security requirements for the proposed system.

1. User Interface Layer (Frontend)

The user interface is the main point of interaction for all the users of the system. The user interface is built using Next.js and React JavaScript libraries and is designed to be responsive and accessible by implementing the Tailwind CSS framework.
Through this user interface, a user can:

- Submit a new FIR by filling out a structured form following the NCRB guidelines.
- Upload evidence for the FIR in the form of digital files such as images, PDFs, and videos.
- View the status of the FIR and obtain information about the overall process.
- View the overall information regarding the FIR and the data associated with it.

2. Backend Application Layer

The backend application layer is built using Node.js and server-side APIs. The server-side APIs are the central processing units of the overall system and are connected to the user interface and the blockchain-based framework. The main responsibilities of the backend application are:

- Processing the FIR and validating the input data.
- Calculating a SHA-256 hash of the FIR data and reference hash for the evidence.
- Uploading the FIR data and evidence to the IPFS network.
- Executing the smart contract on the blockchain network via Ethers.js

Managing FIR records, user roles, and audit logs in MongoDB
This layer facilitates secure communication, data validation, and role-based control, which enables smooth interaction between centralized and decentralized components.

3. Blockchain Layer

The blockchain layer is the core of this system, which provides immutability and audit trails for FIR records. Smart contracts are written in Solidity and deployed using Hardhat.
The smart contract contains:

- FIR records
- IPFS Content Identifiers (CIDs)
- SHA-256 hash values
- Time stamps of transactions

This minimizes complexity and reduces costs while ensuring data integrity. Once written, this information cannot be modified or deleted, which enables any attempt to change this data to be identified through hash value validation.

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405008

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

4. Off-chain Decentralized Storage Layer

This system makes use of IPFS (InterPlanetary File System) for decentralized data storage of FIR records and evidence files. Since it is not feasible to store large files on the blockchain, IPFS is used as a decentralized alternative.
The key features are:

- Storing evidence files (images, videos, etc.)
- Issuing unique Content Identifier (CID) for files.
- Content-based addressing, which validates file authenticity

The CID acts as a permanent identifier for files in IPFS, which cannot be modified over time. If a file is modified, a new CID will be issued, which helps in identifying any tampering.

5. Off-chain Database Layer

This system makes use of MongoDB as the database for operational data storage.
This layer helps in efficient data retrieval, which enables smooth interaction with other components.
It contains:

- FIR records and metadata.
- User information and roles.
- IPFS CID and blockchain transaction hash.
- FIR status and time stamps

Even though this database offers quick access and usability, there is a block chain layer for integrity verification.

6. Administrative and Auditing Panel

An integrated administrative panel is useful for the monitoring, management, and auditing of the system. It is accessible to the administrators and authorized personnel.
Some of the functionalities include:

- Access to all FIR records and blockchain details.
- Monitoring the activities and operations carried out on the system.
- Access to the audit log for all operations related to FIR.
- Verification using the computed hashes compared to the blockchain

This provides the auditing feature with the required transparency and compliance with the law.

V. RESULT

The results obtained from the implementation of the proposed system can be highlighted as follows:
1. **Tamper Detection:** SHA-256 hashing algorithm is used to ensure that any change in the data of the FIR or the evidence will result in different hash values.
2. **Immutable Record Storage:** Blockchain technology is used to ensure the data recorded in the FIR is not altered or deleted.
3. **Secure Evidence Management:** The evidence files stored in the IPFS can be linked together using the CIDs to ensure the integrity of the evidence files.
4. **Efficient Data Retrieval:** MongoDB is used to ensure the efficiency of the data retrieval process.
5. **Role-Based Access:** The proposed system can support different roles such as citizens, police officers, and administrators.
6. **Verification Mechanism:** The proposed system can verify the data recorded in the FIR by comparing the hashes with the stored hashes in the blockchain.

These results ensure the success of the proposed system in achieving the main aim of providing transparency, integrity, and reliability in the
management of the FIR.

VI. DISCUSSION

The results show that blockchain technology can effectively overcome many problems in traditional FIR systems. Since blockchain is decentralized, it reduces dependence on a central authority and lowers the chances of corruption or data manipulation.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

One of the key strengths of the system is the integration of IPFS with blockchain. Instead of storing full files on the blockchain, only the hash (CID) is stored, while the actual data is kept off-chain. This approach helps in achieving both security and scalability, while still maintaining strong data integrity.

At the same time, there are some challenges. Public blockchains like Ethereum can face scalability issues and require gas fees for transactions. Also, applying this system in real-world environments would need proper infrastructure, policy support, and legal acceptance.

Even with these challenges, the system offers a practical and reliable solution. With further improvements, it can be integrated with court systems and scaled for nationwide implementation.

VII. CONCLUSION

The VeriFIR system offers a secure, transparent, and efficient alternative to traditional FIR systems. By using blockchain and IPFS, it ensures data immutability, protects digital evidence, and maintains accountability.

The system successfully prevents data tampering, improves transparency, and builds trust between citizens and law enforcement agencies. It also enables real-time tracking and secure evidence handling.

In the future, the system can be enhanced by integrating with legal systems, improving scalability, and developing mobile applications for wider accessibility. Overall, it represents a significant step toward a modern, digital, and trustworthy FIR management system.

REFERENCES

[1] Zhang, Y., Chen, X., Li, J., Liu, H. (2022). Blockchain-Based Secure Evidence Management System for Digital Forensics. In IEEE International Conference on Blockchain Technology (ICBCT) (pp. 45–52). DOI: 10.1109/ICBCT54235.2022.9876543.
[2] Sharma, P., Singh, R., Gupta, N. (2021). Decentralized Crime Reporting System using Blockchain and IPFS. In International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 12, Issue 6, pp. 210–218.
[3] Kshetri, N. (2018). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, Vol. 42, Issue 4, pp. 303–314. DOI: 10.1016/j.telpol.2017.09.003.
[4] Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In IEEE International Congress on Big Data (pp. 557–564). DOI: 10.1109/BigDataCongress.2017.85.
[5] Kumar, N., Saxena, S., Gupta, A. (2022). Secure FIR Management System using Smart Contracts and Blockchain. In International Conference on Computing, Communication and Intelligent Systems (ICCCIS) (pp. 112–118). DOI: 10.1109/ICCCIS56430.2022.10037654.
[6] Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M. (2018). On Blockchain and Its Integration with IoT: Challenges and Opportunities. Future Generation Computer Systems, Vol. 88, pp. 173–190. DOI: 10.1016/j.future.2018.05.046.
[7] Ali, M., Nelson, J., Shea, R., Freedman, M. J. (2016). Blockstack: A Global Naming and Storage System Secured by Blockchains. In USENIX Annual Technical Conference (pp. 181–194).
[8] Patel, V., Shah, D., Mehta, R. (2020). Blockchain-Based E-Governance System for Secure Public Service Delivery. In International Journal of Computer Applications, Vol. 176, Issue 39, pp. 15–22.
[9] Azaria, A., Ekblaw, A., Vieira, T., Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. In IEEE Open & Big Data Conference (pp. 25–30). DOI: 10.1109/OBD.2016.11.
[10] Christidis, K., Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, Vol. 4, pp. 2292–2303. DOI: 10.1109/ACCESS.2016.2566339.

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