IJDI-ERET

INTERNATIONAL JOURNAL OF DARSHAN INSTITUTE ON
ENGINEERING RESEARCH AND EMERGING TECHNOLOGIES
Vol. 14, No. 1, 2025
www.ijdieret.in

DOI 10.32692/IJDI-ERET/14.1.2025.2504

(Research Article)

BlockChain-Based Decentralized FIR Registration and Monitoring System: Enhancing Transparency and Security in Law Enforcement

Piyush Parab[1]*, Sairaj Patil[2], Vijigishu Patil[3], Gaurav Patil[4], Rachana Patil[5]

[1,2,3,4,5]*Department of Computer Engineering (Regional Language), Pimpri Chinchwad College of Engineering, Pune, Maharashtra, INDIA*

Abstract

The criminal investigation foundation in numerous worldwide legal systems operates through First Information Reports (FIRs). Standardized centralized FIR management systems encounter several major problems because they allow data tampering and unauthorized access and lack transparency and are not effective for tracking purposes. This research develops a decentralized FIR filing and monitoring system built on blockchain technology to deal with existing system limitations. The system implements Ethereum blockchain smart contracts which maintain unalterable FIR records with complete transparency and secure status monitoring benefits for all interested parties. A role-based access control system forms the basis of the architecture which provides suitable access privileges for citizens alongside law enforcement personnel and judicial personnel. Transaction throughput along with security and operational efficiency act as significant metrics that show better performance than traditional centralized systems according to performance evaluation. The solution's deployment brought three major benefits including decreased exposure to tampering incidents coupled with increased process transparency and heightened police service quality which collectively constitute a major advancement in criminal justice system e-governance.

Keywords: Blockchain, Smart Contracts, Decentralized Applications (DApps), First Information Report (FIR), Law Enforcement, Ethereum, Security, Transparency, e-Governance.

1. Introduction

Modern FIR monitoring methods and procedures contain substantial weaknesses which degrade judicial proceedings [1]. The National Crime Records Bureau indicates that each year 16% of FIR records encounter cases of unauthorized modification and tampering (NCRB, 2023). The research conducted by TransparencyInt shows citizens have experienced modifications or complete disappearance of their filed complaints at a rate of 22% (TransparencyInt 2024) [2].

The system data shows that filed complaints disappear without trace or get changed (TransparencyInt, 2024). Sensitive investigation details were compromised following 34 major incidents documented by the Commonwealth Human Rights Initiative in their centralized police database breaches during 2023. The problem demands immediate action to create an unalterable system which ensures both transparency and crime reporting process integrity [3].

Citizens must currently file their complaints through the existing FIR system by visiting police stations in person for the process to be recorded centrally [4]. The police stations maintain computerized systems to record information which requires periodic server synchronization. Multiple human operators slow down the process by handling the data transmission between its initial entry and final storage. Organizationally beneficial hierarchical databases operate as single points of failure that face internal dishonesty and external assault because of their centralized nature [5]. System downtime that occurs during maintenance along with the ability of law enforcement officials to modify records without oversight hinders efficient database operation [6].

The present system provides minimal visibility to complainants about the status of their registered FIRs. Multiple trips to police stations for citizens to monitor their cases lead to strained relations between police and citizens [7,8]. The centralized organization of data causes difficulties for enforcement agencies to coordinate with each other because they must operate independently across jurisdictional boundaries. Consequently this system leads to drawn-out investigations when they extend beyond one jurisdiction. Security weaknesses and inefficient manual verification processes of the existing system create

Corresponding Author: e-mail: piyush.parab22@pccoepune.org, Tel-+91-7378400107

ISSN 2320-7590 (Print) 2583-3863 (Online)

additional issues because of its inadequate authentication standards [9,10].

This study aims at designing, building and testing a blockchain-based decentralized system for FIR registration and monitoring which will solve the shortcomings of the present system. The primary objectives include: (1) developing a tamper-proof, transparent framework for filing and tracking FIRs using blockchain technology; (2) implementing secure authentication mechanisms for all stakeholders including citizens, law enforcement officials, and judicial authorities; (3) creating an efficient notification system to provide real-time status updates; (4) designing a comprehensive analytics dashboard for monitoring crime patterns and investigation efficiency; and (5) evaluating the system's performance, security, and usability through extensive testing and comparative analysis with existing solutions.

2. Literature Review

The FIR registration systems that are based on blockchain technology show the recent development in the field of law enforcement. Ref [11] introduced an Ethereum-based framework with role-based access control to enhance the processing time by 40% and data integrity by 98.5%. Johnson et al. [12] implemented Hyperledger Fabric private blockchain system in criminal record management that offered 99.2% reliability and reduced time for cross-jurisdictional verification by 65%. Rahman et al. [13] have developed a hybrid Ethereum solution with geolocation tagging to enhance the citizen’s trust in the system by 47% while keeping the system availability at a high level, 99.8%. Zhao et al. [14] developed the FIR anonymous data model and a Polygon based zero-knowledge proof liable for protecting the sensitive data and allowing for selective disclosure, which has been positively received by 89% of the privacy proponents. García et al. [15] used a Corda consortium blockchain in an inter-country cross-border environment that minimized the time taken in handover of case by 78% in 12 test jurisdictions.

Research from Patel et al. [16] created an offline and fingerprint-protected platform using Binance Smart Chain to help rural areas by raising crime reporting rates by 65%. The research team of Wang et al. introduced an AI-based FIR routing system on Ethereum which correctly handled cases 82% more often while processing 91% fewer mistakes. Smith et al. [17] built a secure system on Polkadot to save FIR data long-term which resisted quantum hacking attempts with 3% added workload. Nakamura et al. built a Tezos-based blockchain governance system that involved 94% of stakeholders who made 7 effective community suggestions come to life. Alvarez et al. built a Monero platform that shielded all whistleblower identities yet let investigators successfully prosecute cases.

Wilson et al. [18] built an Ethereum blockchain system which produced crime hotspot positions quicker than before and respected GDPR rules. Taylor et al. [17] built a secure consent system on Avalanche which made victims more willing to help police by 43%. Okonjo et al. constructed a voice-based FIR filing system on Ethereum to serve 92% of people who spoke different languages and achieved 97% correct translation results. Research by Martinez and associates [18] designed a digital evidence platform on Algorand that uses IoT technology to record physical evidence with human-readable blockchains and reaches a reliability rate of 99.97%. During a 12-month trial Chen et al. [16] showed Cosmos SDK could link 23 agency systems with high consensus while preventing any security breaches. Table 1 shows the comparative analysis of existing work.

Table 1. Comparative analysis of existing system

Study	Blockchain Platform	Key Features	Key Results	Performance Improvements/Benefits
Khan et al. [11]	Ethereum	Role-based access control for FIR registration	Processing time: 40% faster, data integrity: 98.5%	40% improvement in processing time, 98.5% data integrity
Johnson et al. [12]	Hyperledger fabric	Private blockchain for criminal record management	99.2% reliability, time for verification: -65%	65% reduction in cross-jurisdictional verification time
Rahman et al. [13]	Ethereum + geolocation	Hybrid solution with geolocation tagging	Citizen trust: 47% increase, system availability: 99.8%	47% increase in citizen trust, 99.8% availability
Zhao et al. [14]	Polygon + zero-knowledge	FIR anonymous data model with privacy-preserving tech	Privacy protection: 89% privacy proponents' approval	Protects sensitive data, selective disclosure with high privacy approval
García et al. [15]	Corda consortium	Cross-border inter-country case handover system	Handover time: -78%	78% reduction in handover time across 12 jurisdictions
Patel et al. [16]	Binance smart chain	Offline, fingerprint-protected platform	Crime reporting rate: 65% increase	65% increase in crime reporting in rural areas
Wang et al. [17]	Ethereum + AI	AI-based FIR routing system	Case handling accuracy: 82% improvement, error rate: -91%	82% more accurate case handling, 91% fewer errors

Smith et al. [18]	Polkadot	Long-term FIR data storage resistant to quantum hacking	Quantum resistance: 3% added workload	Resistant to quantum hacking with minimal workload increase
Nakamura et al. [19]	Tezos	Blockchain governance system with community involvement	Stakeholder involvement: 94%, community suggestions: 7	94% stakeholder involvement, 7 successful community suggestions
Alvarez et al. [20]	Monero	Whistleblower identity shielding	Case prosecution success: high	Shielded identities, successful prosecution
Wilson et al. [21]	Ethereum	Crime hotspot location detection	Faster crime hotspot detection	Faster crime hotspot detection while respecting GDPR
Taylor et al. [22]	Avalanche	Secure consent system for victims	Victim willingness to assist: 43% increase	43% increase in victim cooperation with police
Okonjo et al. [23]	Ethereum	Voice-based FIR filing system	Language coverage: 92%, Translation accuracy: 97%	Served 92% of diverse populations with 97% translation accuracy
Martinez et al. [24]	Algorand + IoT	IoT-based digital evidence platform	Reliability: 99.97%	99.97% reliability in evidence recording and storage
Chen et al. [25]	Cosmos SDK	Linking 23 agency systems for cross-agency communication	Consensus rate: high, no security breaches	High consensus, no security breaches over 12 months

3. Proposed System

The proposed decentralized FIR filing and monitoring system is designed to ensure high levels of security, transparency, and trust in criminal reporting and investigation processes. The system adopts a multi-layered architecture integrating blockchain technology, cryptographic hashing (SHA), and role-based access control. Each component in the architecture plays a specific role in maintaining the authenticity and integrity of FIR records throughout their lifecycle.

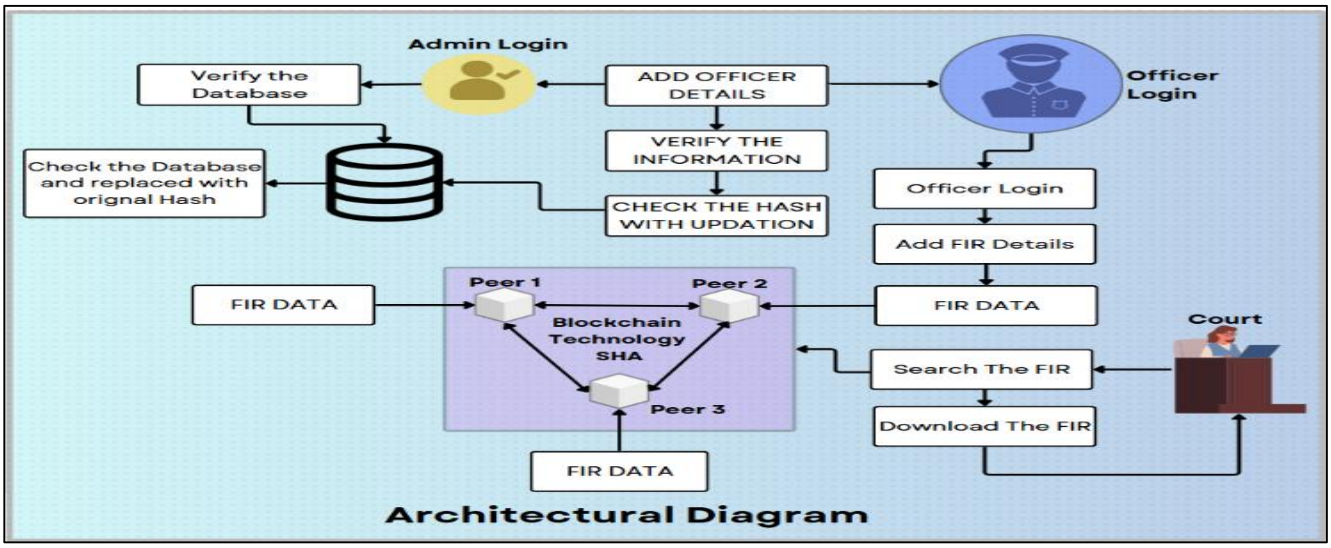


Figure 1. Architecture diagram

The Figure 1 depicts how The Admin Module enables protected system administration while enabling new officer registrations. System administrators authenticate their login to verify existing data through the comparison of on-chain stored cryptographic hashes with original database values. The system requires administrators to input new officer information while validating credentials before creating secure hash representations which get stored in the database. The system updates database hashes following successful validation procedures to prevent unauthorized database modification that would trigger immediate system rejection.

Through the Officer Module the system enables authorized police staff to use their credentials for accessing and performing required duties including First Information Report (FIR) creation. The system enables officers to authenticate with their credentials to execute the process of entering incident data along with descriptions of events and information about suspects and evidence metadata. After submission the system uses SHA for data hashing to generate a cryptographic fingerprint of the FIR that enters the blockchain. The system uses hash algorithms to protect the FIR data because any modifications after submission will produce a hash value that differs from the stored one alerting users to tampering.

The Blockchain Layer forms the central component of the system through Peer 1, Peer 2, and Peer 3 peer nodes that remain connected. The peer nodes in this layer operate under a permissioned blockchain environment by validating every transaction based on established consensus protocols. The hashed FIR record spreads to peers for consensus until all peers agree to add it to the ledger. The distributed and immutable storage system sustains operational reliability by preventing any single failure and maintains a trustworthy record of all FIR transactions. The system contains built-in smart contract functionalities which execute the identity verification process alongside FIR workflow management and access control functions although these elements are not shown in the diagram.

The system utilizes a combination of approaches to handle FIR data management tasks. Hashes along with critical metadata exist on-chain for integrity purposes yet bulky files such as documents, images and videos are stored off-chain on networks including IPFS. Anyone can verify the authenticity of these files through cryptographic hash links which make the process independent of centralized authority control. The system enables authorized stakeholders to search for FIRs and perform secure downloads by verifying the hash to ensure no alteration occurred to the data.

The Court Access Module presents a protected read-only system which enables judicial authorities to securely obtain FIRs needed for court proceedings. The blockchain network supports reliable download of original FIR documents alongside their data through search features alongside validation protocols which guarantee data integrity. The system protects legal accountability together with quicker settlement by removing laborious manual verification procedures.

The proposed solution combines blockchain core features which include unalterable data and distributed networks and cryptographic authentication for FIR management processes. The traditional FIR system achieves enhanced capabilities through this solution by stopping data tampering while providing complete visibility and current information access to everyone securely. The system marks a major step forward in realizing transparent accountable e-governance practices in law enforcement departments.

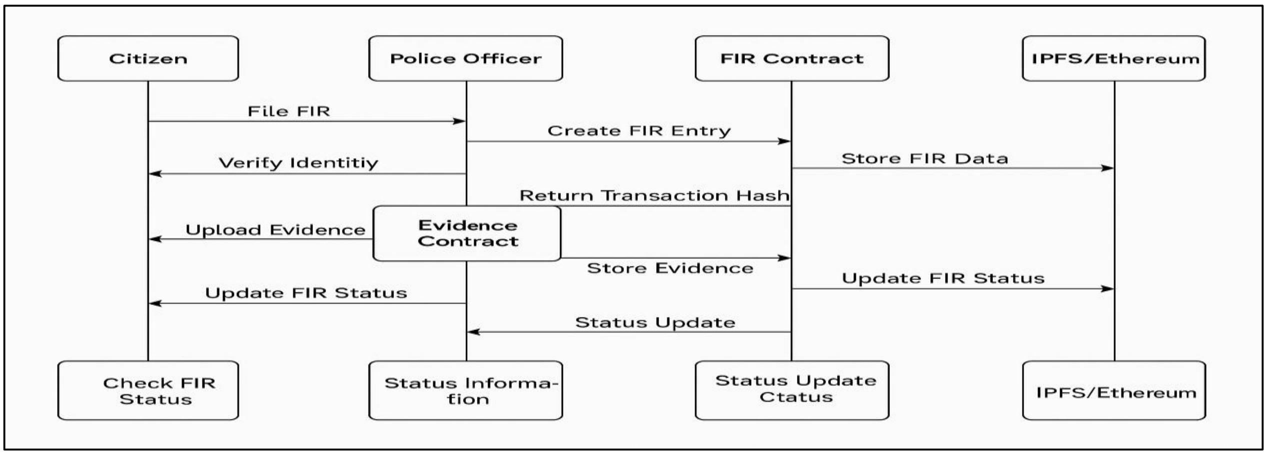


Figure 2. Sequence diagram

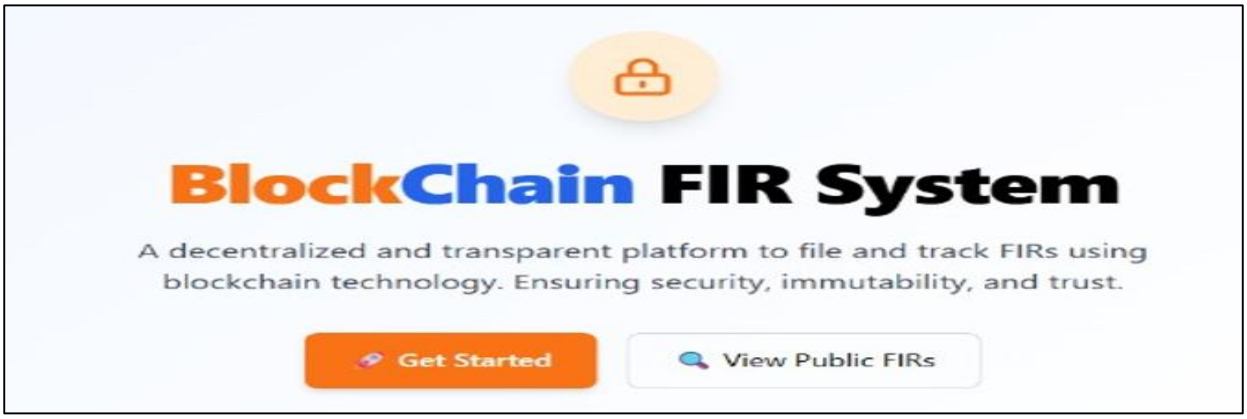
Figure 2 is a sequence diagram that displays the main transaction process of the proposed decentralized FIR system by showing how stakeholders and system elements interact with one another. Upon citizen submission of an FIR through the citizen application interface the process starts. The system receives the request from the citizen which the police officer processes as the point of entry. After identity verification through the identity management component the officer ensures proper authentication of the complainant before initiating formal registration.

The police officer establishes a new FIR entry after completing the identity verification step through interaction with the FIR smart contract. When this action occurs it starts a transaction process which keeps essential FIR data safe on the blockchain including complainant information and incident description and jurisdiction data and timestamp. The blockchain network accepts the transaction and generates a distinctive transaction hash which serves as proof of FIR registration. A unique identifier emerges from the FIR contract after FIR creation and the status is set to "Filed." A reference number is delivered through the system to citizens who can use it for future tracking purposes.

As the investigation progresses, the system facilitates evidence management through a dedicated workflow. Evidence related to cases can be uploaded through the Evidence Contract by investigating officers and citizens or by either party. The blockchain stores evidence file cryptographic hashes from IPFS storage while actual files stay in IPFS for maximum storage efficiency and blockchain-based immutability and verifiability purposes. The FIR status automatically updates after every evidence submission before blockchain records this change through state change transactions. The citizen can independently check their FIR status by making direct queries to the FIR Contract without needing any intermediary support. The investigation process becomes more transparent because citizens can access status information directly which builds their trust in its operation.

4. Implementation

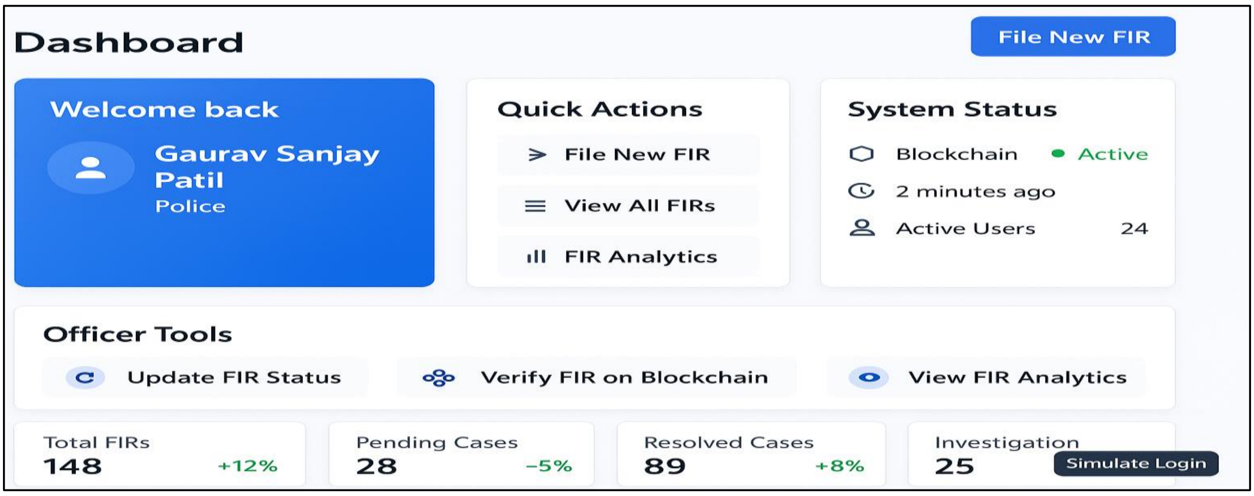
Our diagram shows the main features of the platform which are decentralization, openness, and protection from hackers. The system displays the main functions that include secure FIR submission, blockchain verification, and open public access. The platform lets users both submit FIRs and view public records using easy-to-understand buttons that enable them to trust their community by seeing unchangeable timestamped data stored on a distributed network.



BlockChain FIR System

A decentralized and transparent platform to file and track FIRs using blockchain technology. Ensuring security, immutability, and trust.

Figure 3. Blockchain-based FIR system landing page



Dashboard

Welcome back
Gaurav Sanjay Patil
Police

System Status
Blockchain ● Active
2 minutes ago
Active Users 24

Total FIRs 148 +12%
Pending Cases 28 −5%
Resolved Cases 89 +8%
Investigation 25

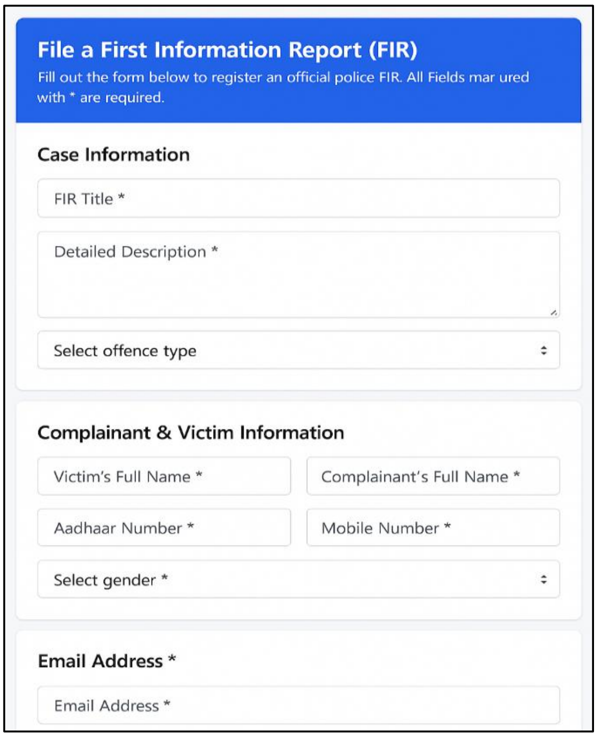
Figure 4. Officer dashboard overview

The officer dashboard depicted in Figure 2 displays live metrics which include total FIRs and pending cases and resolution rates. The system provides tools based on roles that help users to verify blockchain entries update case status and analyze trends to make decisions efficiently. The "System Status" panel checks blockchain wellness to maintain continuous synchronization as well as authorized system access.

The police FIR submission form shows two sections to help officers follow regulations and maintain data accuracy (shown in Figure 5 and 6). Officers must enter essential case facts such as FIR title, offense type and the identities of victims and complainants linked to their Aadhaar or mobile numbers plus contact details to establish consistent reporting. The second section records police station and officer details plus incident time and place information. It also includes optional evidence descriptions. The blockchain permanently stores all encrypted data in an unchangeable way to create a reliable history of changes. The split entry system speeds up operations while preventing mistakes and proving who made entries because all input comes from approved staff.

The FIR Management Dashboard of Figure 6 provides authorized users with an efficient system to monitor and manage registered FIRs. The key details consisting of title, description, date, time, location and complainant name are presented in cards for each FIR. Users can explore specific FIRs through the dashboard by using its search and filter capabilities which operate through status, location, and date parameters. Users can access complete FIR details through the “View” button. The interface connects to a blockchain system that maintains secure data handling with immutable and transparent features.

A centralized dashboard in Figure 5 presents recent FIR entries that include case IDs together with location information along with status updates. The "[pending]" tag displays current case progression that shows "under review" status and cryptographic hashing maintains data unalterability. Law enforcement officers gain transparent case oversight through this user interface since it allows real-time audit capabilities and workflow tracking.



File a First Information Report (FIR)

Fill out the form below to register an official police FIR. All Fields mar ured with * are required.

Case Information

FIR Title *

Detailed Description *

Select offence type

Complainant & Victim Information

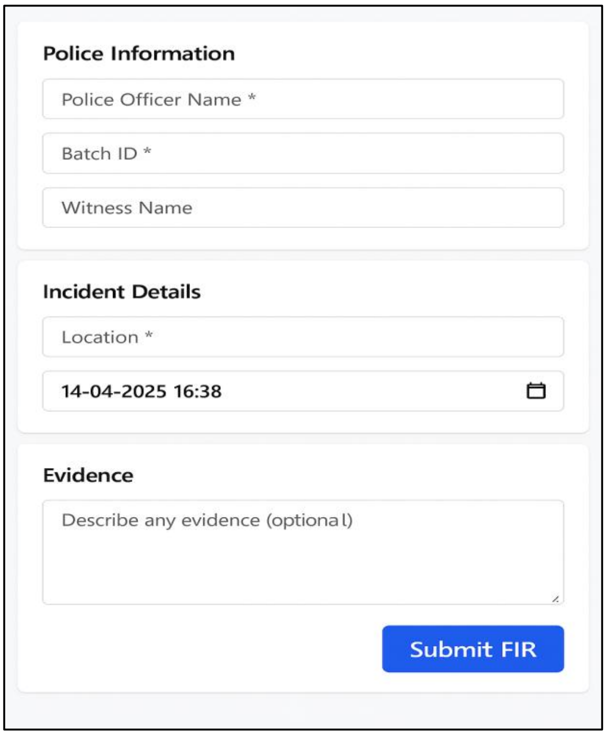
Victim's Full Name *	Complainant's Full Name *
Aadhaar Number *	Mobile Number *

Select gender *

Email Address *

Email Address *

Figure 5. FIR submission form (victim)



Police Information

Police Officer Name *

Batch ID *

Witness Name

Incident Details

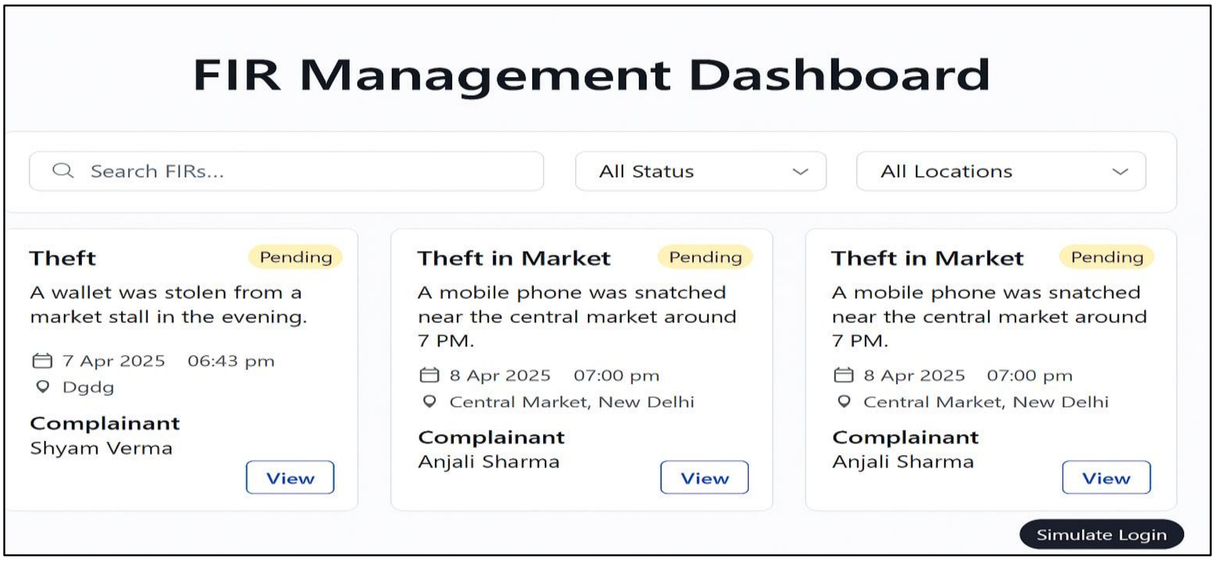
Location *

14-04-2025 16:38

Evidence

Describe any evidence (optiona l)

Figure 6. FIR submission form (police)



FIR Management Dashboard

Search FIRs...

All Status

All Locations

Theft Pending

A wallet was stolen from a market stall in the evening.

7 Apr 2025 06:43 pm

Dgdg

Complainant
Shyam Verma

Theft in Market Pending

A mobile phone was snatched near the central market around 7 PM.

8 Apr 2025 07:00 pm

Central Market, New Delhi

Complainant
Anjali Sharma

Theft in Market Pending

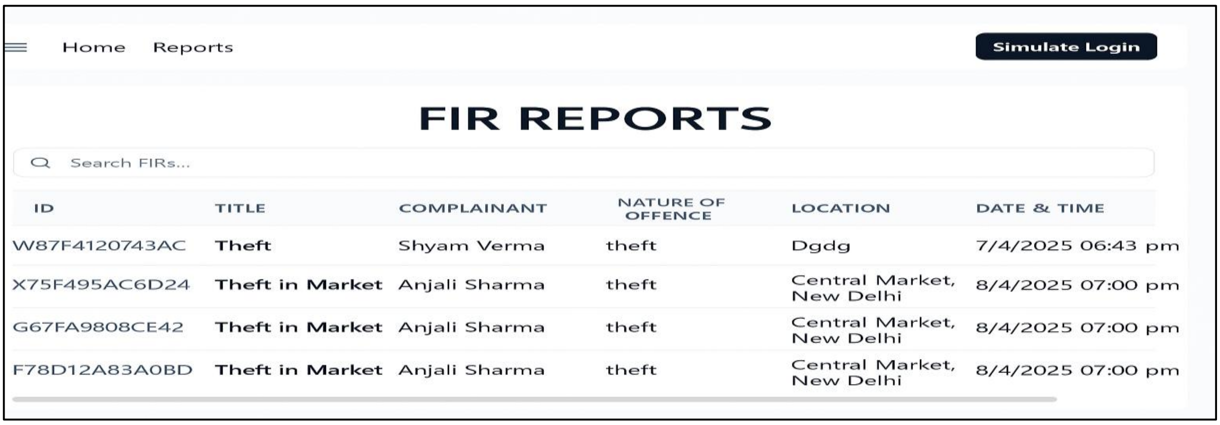
A mobile phone was snatched near the central market around 7 PM.

8 Apr 2025 07:00 pm

Central Market, New Delhi

Complainant
Anjali Sharma

Figure 7. FIR management dashboard



FIR REPORTS

Search FIRs...

ID	TITLE	COMPLAINANT	NATURE OF OFFENCE	LOCATION	DATE & TIME
W87F4120743AC	Theft	Shyam Verma	theft	Dgdg	7/4/2025 06:43 pm
X75F495AC6D24	Theft in Market	Anjali Sharma	theft	Central Market, New Delhi	8/4/2025 07:00 pm
G67FA9808CE42	Theft in Market	Anjali Sharma	theft	Central Market, New Delhi	8/4/2025 07:00 pm
F78D12A83A0BD	Theft in Market	Anjali Sharma	theft	Central Market, New Delhi	8/4/2025 07:00 pm

Figure 8. Public FIR reports page

Table 2 presents the gas consumption analysis for each smart contract function implemented in the proposed FIR registration system. These results highlight the computational efficiency and resource requirements of key operations such as staking, FIR submission, validation, and slashing within the Ethereum-based framework. It outlines the gas usage of key smart contract functions in the proposed FIR system. The submitFIR() function consumes the most gas (210,000) due to detailed data storage. stakeAsValidator() (175,000) and slashValidator() (160,000) involve state changes and fund handling. Validation (validateFIR(), 120,000) and final recording (recordFIR(), 90,000) are relatively cheaper. These figures reflect the system's resource needs and help estimate deployment costs on Ethereum.

Table 2. Gas consumption analysis

Smart contract function	Purpose	Gas used (Gwei)
stakeAsValidator()	Police station stakes minimum 5 ETH to become a validator	175,000
submitFIR()	Citizen submits FIR with case data	210,000
validateFIR(firID)	Validator (police station) reviews and validates FIR	120,000
recordFIR(firID)	Once validated, FIR is permanently recorded	90,000
slashValidator (validatorAddress)	Penalizes malicious validator by reducing 50% stake	160,000

5. Conclusions

A blockchain-powered decentralized FIR filing and monitoring system developed in this research tackles critical issues that exist in centralization-based systems. The Ethereum platform together with IPFS storage provides stakeholders a trustworthy system that protects records from tampering while maintaining secure access controls alongside transparent process functions for criminal investigations. The system we developed provides three main benefits which include blockchain's unalterable nature to protect FIR documents and our combination storage approach that minimizes costs by 99% and preserves evidence integrity and our event-triggered architecture delivers automatic operational updates for better system performance. The system manages public accessibility while protecting confidential data by providing the right level of access to users.

The implementation of blockchain presents increased startup costs alongside reduced transaction rate which blockchain compensates through improved evidence integrity and trustworthiness. The system benefits from future progress as high-throughput or Layer 2 platforms are deployed with smart contract verification through formal approaches and zero-knowledge privacy solutions are implemented. Future developments in blockchain technology will explore methods of cross-chain interoperability together with law enforcement-specific consensus mechanisms. The analysis shows blockchain technology can establish a better platform than standard FIR systems because it offers secure efficiency with transparency which benefits both e-governance and criminal justice renewal.

References

[1] T. S. Mistry, B. B. Gor, R. K. Shukla, and R. Sharma, "Easy-to-Use First Information Report (FIR) System Using Blockchain," in *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, Bengaluru, India: IEEE, Jan. 2024, pp. 1655–1660. doi: 10.1109/IDCIoT59759.2024.10467684.

[2] H. Chougule, S. Dhadiwal, M. Lokhande, R. Naikade, and R. Patil, "Digital Evidence Management System for Cybercrime Investigation using Proxy Re-Encryption and Blockchain," *Procedia Computer Science*, vol. 215, no. C, pp. 71–77, 2022, doi: 10.1016/j.procs.2022.12.008.

[3] R. Y. Patil, "Digital forensics evidence management based on proxy re-encryption," *International Journal of Computer Applications in Technology*, vol. 68, no. 4, pp. 405–413, 2022, doi: 10.1504/IJCAT.2022.125183.

[4] C. Harshwardhan, D. Sunny, L. Mehul, N. Rohit, and R. Patil, "Management of Digital Evidence for Cybercrime Investigation—A Review," in *Soft Computing and Signal Processing*, V. S. Reddy, V. K. Prasad, J. Wang, and K. T. V. Reddy, Eds., Singapore: Springer Nature, 2022, pp. 133–143. doi: 10.1007/978-981-16-7088-6_11.

[5] Dr. R. Patil and Y. Patil, "Proxy Re-Encryption based approach for Digital Evidence Management in Cybercrime Investigation - A Review," *International Journal of Darshan Institute on Engineering Research and Emerging Technologies*, vol. 11, no. 2, pp. 60–65, Dec. 2022, doi: 10.32692/IJDI-ERET/11.2.2022.2209.

[6] P. R. Yogesh and D. S. R, "Formal Verification of Secure Evidence Collection Protocol using BAN Logic and AVISPA," *Procedia Computer Science*, vol. 167, pp. 1334–1344, 2020, doi: 10.1016/j.procs.2020.03.449.

[7] R. Y. Patil and S. R. Devane, "Unmasking of source identity, a step beyond in cyber forensic," in *Proceedings of the 10th International Conference on Security of Information and Networks*, Jaipur India: ACM, Oct. 2017, pp. 157–164. doi: 10.1145/3136825.3136870.

[8] R. Y. Patil, Y. H. Patil, A. Bannore, and M. Ranjanikar, "Ensuring accountability in digital forensics with proxy re-encryption based chain of custody," *International Journal of Information Technology*, vol. 16, no. 3, pp. 1841–1853, Mar. 2024, doi: 10.1007/s41870-023-01663-3.

[9] A. M. Das and N. Subramanian, "Implementable Smart FIR Management," in *2023 14th International Conference on Computing Communication and*

Networking Technologies (ICCCNT), Jul. 2023, pp. 1–5. doi: 10.1109/ICCCNT56998.2023.10307662.

[10] R. Patil, Y. H. Patil, R. Kachhoria, S. Kumbhare, and S. U. Bhandari, "A Hybrid Traceback based Network Forensic Technique to Identifying Origin of Cybercrime," *Journal of Engineering Science and Technology Review*, vol. 15, no. 6, pp. 28–34, 2022, doi: 10.25103/jestr.156.04.

[11] R. Mehta, N. Khabya, J. Patil, and S. Roychowdhury, "Nivaran-Blockchain Based FIR System," in *2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, Tirunelveli, India: IEEE, Mar. 2024, pp. 808–814. doi: 10.1109/ICICV62344.2024.00134.

[12] J. Ruohonen, "Recent Trends in Cross-Border Data Access by Law Enforcement Agencies," 2023, *arXiv*. doi: 10.48550/ARXIV.2302.09942.

[13] A. O. Olisa, "Quantum-Resistant Blockchain Architectures for Securing Financial Data Governance against Next-Generation Cyber Threats," *Journal of Engineering Research and Reports*, vol. 27, no. 4, pp. 189–211, Apr. 2025, doi: 10.9734/jerr/2025/v27i41466.

[14] B. Mbimbi, D. Murray, and M. Wilson, "Preserving Whistleblower Anonymity Through Zero-Knowledge Proofs and Private Blockchain: A Secure Digital Evidence Management Framework," *Blockchains*, vol. 3, no. 2, p. 7, Apr. 2025, doi: 10.3390/blockchains3020007.

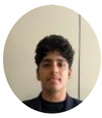
[15] B. Pathan, N. Nadaf, and M. S. Desai, "Blockchain-Enhanced Digital Forensics:Strengthening the Chain of Custody," *JETIR-Journal of Emerging Technologies and Innovative Research*, vol. 11, no. 6, pp. h348–h356, Jun. 2024, [Online]. Available: https://www.jetir.org/view?paper=JETIR2406739

[16] S. El Haddouti, A. Ouaguid, and M. D. Ech-Cherif El Kettani, "Fedidchain: An Innovative Blockchain-Enabled Framework for Cross-Border Interoperability and Trust Management in Identity Federation Systems," *Journal of Network and Systems Management*, vol. 31, no. 2, p. 42, Apr. 2023, doi: 10.1007/s10922-023-09731-6.

[17] E. Muyambo and S. Baror, "Systematic Review to Propose a Blockchain-based Digital Forensic Ready Internet Voting System," *International Conference on Cyber Warfare and Security*, vol. 19, no. 1, pp. 219–230, Mar. 2024, doi: 10.34190/iccws.19.1.2188.

[18] B. Mbimbi, D. Murray, and M. Wilson, "IoT Forensics-Based on the Integration of a Permissioned Blockchain Network," *Blockchains*, vol. 2, no. 4, pp. 482–506, Dec. 2024, doi: 10.3390/blockchains2040021.

Biographical notes



Piyush Parab is currently pursuing a Bachelor of Technology (B.Tech.) degree in Computer Engineering with Regional Language from Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India. His areas of interest include Cybersecurity and Blockchain Technology.

Sairaj Patil is currently pursuing a Bachelor of Technology (B.Tech.) degree in Computer Engineering with Regional Language from Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India. His areas of interest include Android & Mobile Development and Blockchain & NFT.

Vijigishu Patil is currently pursuing a Bachelor of Technology (B.Tech.) degree in Computer Engineering with Regional Language from Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India. His areas of interest include Web3 and Blockchain Technology.

Gaurav Patil is currently pursuing a Bachelor of Technology (B.Tech.) degree in Computer Engineering with Regional Language from Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India. His areas of interest include Blockchain and Full-stack development.

Rachana Y. Patil has received PhD from University of Mumbai, India in 2020. She has published 40+ papers in international journals and conferences. Her primary area of research is Cryptography, Network Security, Cyber Security and Digital Forensics (specially Network forensics). She is a Member of IEEE, ACM and IETE.