

E-Fir And Complaints System Using Blockchain

¹Ms. Vishakha Sonawane¹, Prof. Sana Naikwadi², Ms. Sharayu
Lodhe³, Mr. Sumit Najan⁴, Mr. Ketan Wagh⁵

¹Department Of Information Technology ,

¹Information Technology Department/Genba Sopanrao Moze College of Engineering,
Balewadi,Pune/SPPU/India

Abstract: India's shift towards digitalization has transformed traditional manual systems into a centralized online platform for registering complaints. However, the security of the First Information Report (FIR) process remains a significant concern. This paper proposes a solution that utilizes blockchain technology to strengthen the security, traceability, and chronological accuracy of FIR records. The study examines current police case management procedures, explores the potential of blockchain, and discusses an integrated police record management system that incorporates blockchain, Machine Learning (ML), and the Internet of Things (IoT). A key focus of the paper is to propose a mechanism to prevent tampering with e-FIR data, which is vulnerable due to local control. The primary challenges with traditional methods include the lack of trust in e-FIR data, counterfeit registrations, and the risk of non-registrations. These issues stem from corruption, inefficiency, and a lack of transparency. The paper emphasizes the need for a system free from corruption, leveraging blockchain to ensure the integrity of e-FIR data, eliminate fake registrations, and foster a more transparent and reliable reporting system.

Index Terms - Forensic Investigation, Law Enforcement, Blockchain Technology, Cybersecurity, Cryptography, Data Integrity, Security Threats.

I. INTRODUCTION

Information and Communication Technologies (ICT) play a central role in developing smart cities, aiming to enhance the quality of life for residents by promoting economic growth, enabling sustainable governance, optimizing resource management, and ensuring secure mobility. These advancements are achieved while safeguarding the security and privacy of citizens. In a smart city, where systems such as smart cars, schools, hospitals, utilities, and more are interconnected, exchanging vast amounts of data over the internet requires a sophisticated and secure framework, particularly for managing Electronic First Information Report (e-FIR) data within police stations. As the volume of data grows, the importance of accurate record-keeping and efficient information dissemination has become even more critical. Moreover, protecting national security requires reliable, time-stamped records to streamline legal processes and ensure transparency.

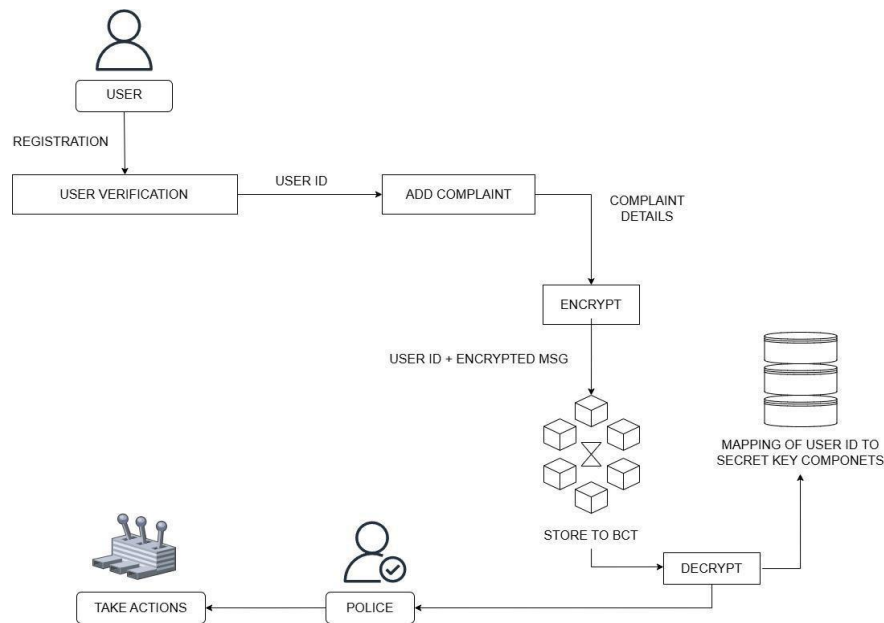
II. LITERATURE REVIEW

1. An Electronic First Information Report (e-FIR) is a critical document submitted to police stations, typically by the victim or their representative, when a cognizable offense occurs. The following outlines various existing methods and challenges associated with FIR filing:

2. **FIR Filing Process:** The FIR serves as the first step in registering a cognizable offense, typically based on the victim's statement, which is subsequently verified by the police.
3. **Investigation and Evidence Collection:** After the FIR is filed, the police officer initiates an investigation at the crime scene, collecting relevant evidence. Following the investigation, a complete case report is submitted to the magistrate. If sufficient evidence is found, a charge sheet is filed; otherwise, a closure report is presented.
4. **Court Proceedings and Bail:** Once the investigation is complete, court proceedings commence. If the police fail to conclude the investigation within 60 to 90 days (depending on the nature of the offense), the accused may be granted bail. It is important to note that the Criminal Procedure Code (CrPC) does not allow the cancellation of an FIR before the completion of the investigation.
5. **Magistrate's Role:** Only after the investigation is concluded can the magistrate, under Section 173(2) of the CrPC, drop proceedings and cancel the FIR.
6. **India's crime rate** has shown a concerning rise, with 51,56,172 cognizable crimes recorded in 2019, including 32,25,701 crimes under the Indian Penal Code (IPC) and 19,30,471 crimes under Special Local Laws (SLL). This marks a 1.6% increase over 2018, with the crime rate per lakh population rising slightly from 383.5 in 2018 to 385.5 in 2019.
7. **Challenges in FIR Filing:** Research by Banerjee et al. in collaboration with the Rajasthan police found that police officers working long hours often face reduced efficiency and job satisfaction, resulting in delays in FIR filing and case processing.
8. **Underreporting and Manipulation of FIRs:** Another report highlighted the issue where officers, in an effort to maintain low crime statistics, may refuse to file certain FIRs, leading to inaccurate data and the denial of justice.
9. **Blockchain Technology for Secure Record Keeping:** Blockchain systems are designed to record data in a chronological, transparent, and traceable manner, with timestamped transactions that cannot be altered once confirmed. These features make blockchain particularly suited for secure information storage and processing.
10. **Blockchain Network Components:** Key components of a blockchain network include cryptography, transactions, consensus mechanisms, and a distributed ledger. Data exchange within the blockchain occurs peer-to-peer between nodes, with each transaction affecting the state of the blockchain.
11. **Blockchain in Smart Cities:** Blockchain technology has been explored for various applications in smart cities, especially for security-related functions. Its inherent reliability makes it a promising solution for establishing a secure framework for governmental and organizational data storage and processing. Several researchers have proposed integrating blockchain into the FIR filing process to enhance data integrity, prevent false FIR registrations, and ensure transparency throughout the system.

III. PROPOSED SYSTEM

The security protocol for safeguarding the FIR system includes the following steps:



Enhanced Security Measures for Blockchain-Based FIR System

1. User Registration and Identity Verification:

To maintain a secure environment, all system users—including complainants, suspects, and witnesses—must complete a registration process through a secure interface. Users provide Aadhaar, email, and mobile number details to confirm their identity and prevent unauthorized access. Each law enforcement officer and investigator is given a unique ID and one-time passwords (OTPs) to ensure secure access to case files and to interact confidentially with other users involved in a case.

2. Complaint Submission and Updates:

Once registered, users can perform various case-related actions based on their role:

- Complainants can:
- Submit new complaints or crime reports.
- Access case information and updates.
- Upload evidence, including multimedia such as images, audio, and video files, which officers can review for verification.
- Comment on case details or respond to evidence, allowing officers to track the source of any questionable information.

3. Data Encryption for Privacy and Security:

To protect FIR information, the system uses cryptographic techniques that securely encrypt all data before it is stored. Blockchain's immutable nature ensures that once data is encrypted and stored, it cannot be altered or tampered with, ensuring data integrity and transparency.

4. Blockchain-Based Record Storage:

FIR records are stored on the blockchain, creating a decentralized and highly secure repository. This technology prevents tampering, enhances transparency, and ensures a permanent and trustworthy record of all criminal reports, reinforcing the integrity of legal documentation.

5. Controlled Decryption for Authorized Access:

Access to sensitive FIR information is controlled through a decryption process that utilizes blockchain's tamper-resistant features. Only authorized personnel can decrypt and view FIR data, preventing unauthorized alterations and safeguarding the information's accuracy and reliability.

6. Secure User Identity and Access Control:

Each user's ID is associated with specific cryptographic keys that are securely stored on the blockchain. This unique mapping system ensures that only verified users can access or update FIR information. With blockchain, access control is transparent and tamper-resistant, preserving secure and verifiable identities for all actions taken within the system.

7. Transparent and Immutable Police Records:

The blockchain-based FIR system provides law enforcement with a reliable way to create and manage secure, tamper-proof records for each FIR. Blockchain's decentralized framework minimizes the risk of data corruption, helping to build public trust in the legal process by offering verifiable and immutable records of all case activities.

8. Streamlined Investigation and Action Steps:

With FIR data stored on a secure, decentralized ledger, law enforcement can collaborate more effectively, as blockchain facilitates authorized data sharing. This secure and tamper-resistant system enhances the speed and reliability of investigations, ensuring transparent and timely actions within the justice system.

IV. EXISTING SYSTEM

The current online system for filing complaints and First Information Reports (FIRs) varies significantly across different states in India, with each state adhering to its own set of regulations and procedures. In some states, online FIR filing may not be available at all, while in others, it is limited to reporting only cognizable offenses. Cognizable offenses, such as murder, rape, dowry death, and kidnapping, can be reported using an e-FIR, allowing police to make arrests without the need for a court warrant. In contrast, non-cognizable offenses like assault, cheating, and harassment can only be reported online, and these reports must be later upgraded to FIRs with approval from a magistrate.

While some states do allow citizens to file their FIRs or complaints online, there are significant concerns regarding the security and integrity of the data within the existing system. In the current framework, all data is stored in centralized databases, and file transfers over the internet are susceptible to tampering. This centralized approach creates vulnerabilities that can compromise the accuracy and authenticity of criminal records.

In the current system, e-FIR data is initially stored locally in a police station's central database before being shared with higher authorities or the station's headquarters. This local handling of data makes it more vulnerable to manipulation. By implementing blockchain technology, these security concerns can be mitigated. Blockchain's decentralized, fraud-resistant ledger system would ensure that FIR data remains secure and tamper-proof. As a distributed ledger, blockchain allows for the reliable tracking and preservation of crimelated information in a way that traditional police station databases cannot, preventing unauthorized alterations and improving the overall transparency of the system.

V. CONCLUSION

The proposed blockchain-based FIR system strengthens the integrity and transparency of case records by addressing limitations in traditional methods. This solution introduces a decentralized approach that prevents tampering, enhances traceability, and promotes accountability within law enforcement. By implementing blockchain, the system ensures that FIR records are secure, traceable, and resistant to unauthorized changes, which can improve public trust in law enforcement processes. Although infrastructural challenges remain, this system lays the groundwork for a more reliable and efficient case management framework in Indian policing.

REFERENCES

1. Alharby, M., & Van Moorsel, A. (2017). "Blockchain-based smart contracts: A systematic mapping study." *Computer Science Review*, 30, 13-18.
2. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." *IEEE International Congress on Big Data*, 557-564.
3. Hasan, H. R., & Salah, K. (2018). "Blockchain-based proof of delivery of physical assets with single and multiple transporters." *IEEE Access*, 6, 46781-46793.
4. Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). "A decentralized privacy-preserving healthcare blockchain for IoT." *Sensors*, 19(2), 326.
5. Kshetri, N. (2017). "Blockchain's roles in strengthening cybersecurity and protecting privacy." *Telecommunications Policy*, 41(10), 1027-1038.

6. Toyoda, K., Mathiopoulos, P. T., Sasase, I., & Ohtsuki, T. (2017). "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain." IEEE Access, 5, 17465-17477.
7. Kumar, N., & Tripathi, R. (2019). "A secure and efficient blockchain-based electronic health record management system." IEEE Access, 7, 77416-77430.
8. Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). "Exploring blockchain technology and its potential applications for education." Smart Learning Environments, 5(1), 1-10.
9. Biswas, K., & Muthukkumarasamy, V. (2016). "Securing smart cities using blockchain technology." 2016 IEEE 18th International Conference on High-Performance Computing and Communications, 1392-1393.
10. Shah, R., & Rathod, N. (2021). "Blockchain and Smart Contracts in Digital Identity Verification." Springer Lecture Notes on Data Engineering and Communications Technologies, 57, 247-260.
11. https://link.springer.com/chapter/10.1007/978-3-031-69201-7_18

