IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CRYPTOSHIELD FIR SYSTEM USING BLOCKCHAIN

[1]Devesh Dhone, [2]Prajkta Elinje, [3]Anushka Chaudhary, [4] Susmita Soma

[1]Prof. Jayshri Mankar

[1]Department of Computer Engineering,
Genba Sopanrao Moze College of Engineering Balewadi, Pune-411045, Maharashtra, India

Abstract: India's digitalization has led to a shift from traditional manual systems to a centralized online process for registering complaints, but the security of the First Information Report (FIR) system remains a critical concern. This paper proposes a solution that leverages blockchain technology to enhance the security of FIRs, addressing the need for a more secure, traceable, and chronological record-keeping system. The paper analyses existing police case-related procedures, the potential of blockchain technology, and proposed systems, including an integrated police record management system that incorporates blockchain, Machine Learning (ML), and the Internet of Things (IoT). The paper also proposes a mechanism to prevent tampering with e-FIR data, which can be compromised due to local control. The main issues with traditional methods include trustworthiness of e-FIR data, counterfeit registrations, and non-registrations. Corruption, inefficiency, and lack of transparency are the underlying causes of these problems. Implementing a system free from corruption is imperative, and blockchain technology is employed to protect the integrity of e-FIR data and prevent fake registrations, ensuring a more transparent and trustworthy system.

Index Terms - Forensic Investigation, Law Enforcement, Blockchain Technology, Cybersecurity, Cryptographic Techniques, Security Breaches.

I. INTRODUCTION:

Information and communication technologies ICT play a pivotal role in the development of smart cities. ICT investments aim to enhance the quality of life for citizens by fostering economic growth, sustainable governance, efficient resource management, and secure mobility. This progress is realized while maintaining the security and privacy of the city's inhabitants. In a smart city where smart cars, schools, hospitals, utilities, and more are interconnected, the exchange of vast data volumes over the internet necessitates a sophisticated and secure framework for handling Electronic First Information Report e-FIR data within police stations. The significance of accurate record-keeping and information dissemination has become

more critical with the expansion of data. Furthermore, the need to safeguard national security calls for trustworthy and time-stamped records to simplify the process. To ensure the security of a smart city, it is essential to comprehend the nuances of classifying offenses. These offenses can be categorized into two groups. Cognizable Offenses These are serious crimes that law enforcement can address without requiring a warrant, including murder, robbery, dowry-related deaths, kidnapping, and more. Trustworthy and time-stamped records simplify the handling of such offenses.

II. LITERATURE REVIEW:

An Electronic First Information Report (e-FIR) serves as a fundamental document submitted to police stations by either the victim or a representative in the event of a cognizable offense. Various existing methods for filing an FIR are explored below:

[1] The First Information Report FIR serves as the initial step in registering a cognizable offense, usually based on the victim's statement, which is later verified by the police.

[2] Subsequently, the police officer initiates an investigation into the crime scene and collects relevant evidence. Following the investigation, a complete case report is submitted to the magistrate. If the offense is established in the report, a charge sheet is filed otherwise, a case closure report is presented.

[3] Court proceedings commence, and if the police fail to complete the investigation within sixty or ninety days depending on the nature of the offense, the accused may be released on bail. Notably, there is no provision in the Criminal Procedure Code CrPC to cancel an FIR before the investigation's completion.

[4] Only after the investigation is concluded can the magistrate, as per 173(2) of the CRPC, drop the proceedings and cancel the FIR. It is concerning that India's rising crime rate led to a total of 51,56,172 cognizable crimes in 2019, comprising 32,25,701 Indian Penal Code IPC crimes and 19,30,471 Special Local Laws SLL crimes, marking a 1. 6 increases over 2018 4. Additionally, the crime rate per lakh population marginally rose from 383. 5 in 2018 to 385. 5 in 2019.

[5] Research conducted by Banerjee et al. In collaboration with the Rajasthan police revealed that police officers who work long hours often experience reduced efficiency and job satisfaction, leading to delays in the FIR process and other case-related proceedings.

[6] Another report highlighted that officer, to maintain low crime figures, may refuse to file certain FIRs, leading to inaccurate data and a lack of justice.

[7] A national survey revealed that citizens confidence in their country's police departments did not rank India among the countries with high confidence levels.

[8] Blockchain systems record data in chronological order, timestamping and storing transactions in a transparent and traceable manner.

[9] Key components of a blockchain network include cryptography, transactions, consensus mechanisms, and the distributed ledger. Information exchange in the blockchain network occurs peer-to-peer through file transfer between nodes, and each transaction changes the blockchain's state.

[10] Blockchain technology has been explored for applications in smart cities, particularly for security-related functions. Its reliability makes it suitable for establishing a secure framework for governmental and organizational information storage and processing. Researchers have proposed various solutions to integrate blockchain technology into FIR filing processes, aiming to enhance data integrity, prevent false FIR registrations, and maintain transparency.

III. PROPOSED METHOD:

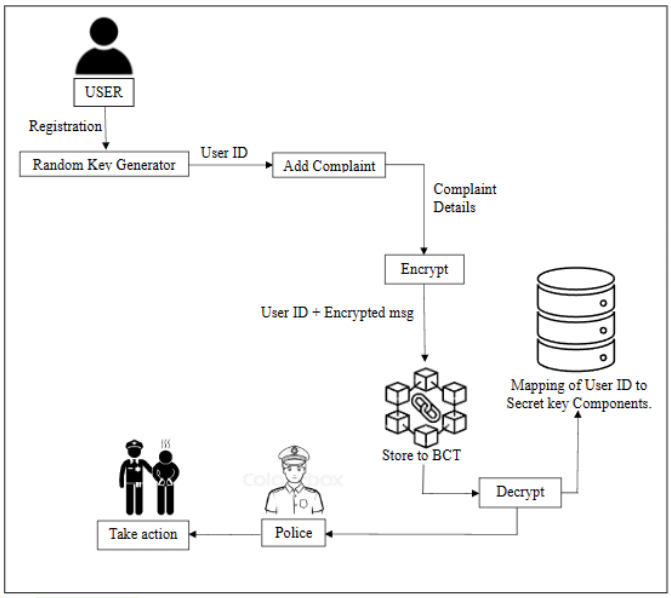

Fig: -System architecture.

The procedure for maintaining security within the FIR system is outlined as follows:

1. User Registration: To ensure the security of the FIR system, all complainants, suspects, and witnesses must register through the User Interface. This registration process acts as a protective measure to verify their identities. Users will be required to provide their AADHAAR CARD for enhanced verification. Officers will be assigned unique IDs to access and manage cases. Investigating officers will also receive unique IDs to collaborate with users, including complainants, suspects, and witnesses.

2. Random Key Generator: After registration, the system will categorize users and provide them with private and public keys to interact with the blockchain for their specific cases. User verification will be carried out by the assigned case officers, whose identities will remain confidential. Users will receive notifications once verification is complete, and the system will remove their access keys after the case is resolved.

3. Add Complaint: Once users have their access keys, they can perform various tasks based on their roles:

a. Complainants:

i. File a complaint regarding a crime.

ii. Retrieve information about the case.

iii. Update case information, including images, voice recordings, videos, or physical evidence submitted to the police station for verification.

iv. Comment on existing evidence. If false information is added, the responsible officers can investigate.

4.Encrypt: Encrypting data for a FIR (First Information Report) system using Blockchain technology involves securing the information within the FIR using cryptographic techniques and storing it on a blockchain for added integrity and transparency.

5. Store to BCT: Implementing blockchain technology in the FIR (First Information Report) system involves creating a decentralized and secure platform to store FIR records. This ensures that the information is tamper-proof and transparent, enhancing the integrity of legal documentation. By leveraging blockchain, authorities can streamline the process, reduce fraud, and provide a reliable and immutable record of criminal incidents.

6. Decrypt: Decrypting for a FIR (First Information Report) system using Blockchain Technology involves utilizing the decentralized and tamper-resistant nature of blockchain to securely access and retrieve sensitive information from FIR databases. Blockchain ensures data integrity and transparency, preventing unauthorized alterations to FIR records. This enhances trust in the system, as the decentralized ledger ensures that information is reliable and accessible only to authorized parties, reinforcing the integrity of the FIR process.

7. Mapping of user ID to secret key components: In a FIR (First Information Report) system utilizing Blockchain Technology, the mapping of user IDs to secret key components is executed through decentralized and tamper-resistant ledgers. Each user's ID is linked to unique cryptographic keys stored on the blockchain, ensuring secure and transparent access control. This distributed approach enhances the system's integrity, making it resistant to unauthorized alterations and providing a trustworthy foundation for maintaining user identity and security within the FIR system.

8. Police: The Police FIR system utilizing Blockchain Technology ensures a secure and tamper-proof record of First Information Reports (FIRs). Blockchain's decentralized and transparent nature prevents data manipulation, enhancing the credibility of FIRs. This innovation promotes trust in law enforcement processes, reduces the risk of data corruption, and streamlines the investigation and judicial procedures by providing a verifiable and immutable digital ledger for FIR documentation.

9. Take Action: Implementing Blockchain Technology in the FIR (First Information Report) system can enhance the accountability and transparency of criminal investigations. By storing FIR data in a decentralized and tamper-resistant ledger, it ensures the integrity of the information, reducing the risk of manipulation. This technology enables secure sharing of data among law enforcement agencies, streamlining the process and promoting swift and effective actions against criminals.

IV. ALGORITHM:

SHA-256, a cryptographic hash function:

SHA-256 is not a form of "encryption" because it produces a fixed-size output regardless of the source text's length, and it cannot be reversed to reveal the original text. Instead, it finds significant utility in scenarios involving data integrity and authentication, allowing for secure data handling without the need to decrypt the information.

This hashing technique serves various purposes, such as:

1. Data Comparison: Hashed versions of texts can be compared without the need for decryption, ensuring data integrity and authenticity.

2. Server Validation: When a client needs to send a password's hash over the internet for server validation, using methods like challenge handshake authentication (or challenge hash authentication) minimizes the risk of the original password being intercepted.

3. Anti-Tampering Measures: By linking a message's hash to the original, recipients can re-hash the message and compare it to the provided hash. If they match, it indicates the message's integrity and verifies that there was no data loss during transmission.

Creating digital signatures for documents is a more intricate process, but it involves hashing the document and encrypting the resulting hash with your private key. Others can then decrypt this signature using your public key to recover the original hash, enabling them to authenticate the text by comparing it to their own hash of the document.

It's crucial to note that hash functions, including SHA-256, are designed for quick computation, making them vulnerable to brute force attacks. Therefore, they are not suitable for storing encrypted passphrases securely. For password storage, it is advisable to use key derivation algorithms like bcrypt and scrypt, which intentionally slow down the hashing process, enhancing security.

V. EXISTING SYSTEM:

The online system for filing complaints and FIRs varies across different states, each adhering to its specific regulations and procedures. In certain states, this online service might not be available at all, while in others, it is limited to reporting cognizable offenses. Cognizable offenses, such as murder, rape, dowry death, kidnapping, and similar serious crimes, can be reported using an e-FIR. In these cases, the police have the authority to make arrests without requiring a court warrant. On the other hand, non-cognizable offenses like assault, cheating, harassment, and similar lesser offenses can only be submitted as reports online. The police

will subsequently upgrade these reports to FIRs upon obtaining approval from a Magistrate. Currently, in some states, you have the option to submit your FIR or complaint online. However, there are concerns about the security and integrity of criminal records in the existing system, as all the data is stored in a centralized node, and internet file transfers are vulnerable to data tampering.

In contrast, blockchain technology provides a secure and tamper-proof solution. Transactions recorded on the blockchain cannot be altered, and any attempt to change data is easily traceable due to the change in the associated hash value. This level of transparency and security is lacking in the current system, where issues like non-registration, false registration, and data integrity of e-FIRs are prevalent.

These problems are often rooted in corruption, inefficiency, a lack of transparency, and a casual approach to the situation. In the current system, e-FIR data is initially stored locally in a police station's central database before being shared with the station's headquarters. This local handling of data can make it susceptible to alterations. By implementing blockchain technology, we can effectively address these security concerns and ensure the integrity of e-FIR data. Blockchain acts as a fraud-resistant, distributed ledger that records all transactions within a Peer-to-Peer (P2P) network. This digital system offers a reliable way to track and preserve crime-related information, a feature currently lacking in traditional police station computer systems, where data may be altered under various circumstances.

VI. CONCLUSION:

In this research, we conducted an in-depth examination of the case record management systems employed by Indian law enforcement agencies. Our investigation encompassed the entire case workflow, identifying the diverse stakeholders involved in the process. We scrutinized the conventional methods of First Information Report FIR registration and case record management, exposing their inherent shortcomings and underscoring the imperative for the introduction of an online system. Furthermore, we explored the subsequent online systems that have been implemented and analysed the optimization proposals put forth by various researchers. It became evident that a modern, unalterable, transparent, accountable, traceable, and chronological system was urgently needed to enhance efficiency and mitigate malpractices within the system. The adoption of blockchain technology, with its inherent mechanisms, architectural features, and diverse components, emerged as a compelling solution for this specific application. Consequently, we delved into a comprehensive review of several blockchain-based systems recently proposed to address these challenges, highlighting both their advantages and drawbacks. However, while these systems have made significant strides in improving operational efficiency and workflows, it is essential to acknowledge that our country, as a developing nation, is still in the process of establishing the necessary infrastructure to support a blockchain-based online system. Challenges associated with aspects such as storage, accessibility, online facilities, and the availability of skilled and trustworthy human resources remain unresolved. The hybrid police record management solutions we propose offer a potent alternative, ensuring an efficient, tamper-proof case management system. Our paper introduces an approach that enables users to file FIRs online, eliminating the need to visit a physical police station. Citizens can directly interact with government authorities, access government information, check the status of their cases, and communicate with higher-

ranking officials, thereby enhancing the relationship between law enforcement and the public, as well as the governments connection with its constituents.

VII. REFERENCES:

[1] Al Omar, Abdullah, Abu Kaisar Jamil, Amith Khandakar, Abdur Razzak Uzzal, Rabeya Bosri, Nafees Mansoor, and Mohammad Shahriar Rahman. "A transparent and privacy- preserving healthcare platform with novel smart contract for smart cities." IEEE Access 9 (2021)

[2] Chen, Zerui, Youliang Tian, and Changgen Peng. "Anincentive-compatible rational secret sharing scheme using blockchain and smart contract. "Science China Information Sciences64 (2021): 1-21.

[3] Jyoti, Amrita, and R. K. Chauhan. "A blockchain and smartcontract-based data provenance collection and storing in cloud environment." Wireless Networks 28, no. 4 (2022): 1541-1562.

[4] A. Kumar, K. Abhishek, P. Nerurkar, M. R. Ghalib, A. Shankar, and X. Cheng, ``Secure smart contracts for cloud- based manufacturing using ethereum blockchain," Trans. Emerg. Telecommun. Technol., vol. 33, no. 4, p. 4129, Apr. 2022.

[5] T. Li, D. Li, and M. Wang, ``Blockchain-based fair and decentralized data trading model," Comput. J., vol. 65, no.8, pp. 2133_2145, Aug. 2021.

[6] T. Li, W. Ren, and Y. Xiang, `" FAPS: A fair, autonomous and privacy preserving scheme for big data exchange based on oblivious transfer, ether cheque and smart contracts," Inf. Sci., vol. 544, pp. 469_484, Feb. 2021.

[7] Lin, Chao, Debiao He, Xinyi Huang, and Kim-Kwang Raymond Choo. "OBFP: Optimized blockchainbased fair payment for outsourcing computations in cloud computing." IEEE Transactions on Information Forensics and Security16 (2021): 3241-3253.

[8] W. Xiong and L. Xiong, ``Anti-collusion data auction mechanism based on smart contract,"Inf. Sci., vol. 555, pp.386_409, May 2021.

[9] Xuan, Shichang, Li Zheng, Ilyong Chung, Wei Wang, Dapeng Man, Xiaojiang Du, Wu Yang, and Mohsen Guizani. "An incentive mechanism for data sharing based on blockchain with smart contracts." Computers & Electrical Engineering 83 (2020): 106587.

[10] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, and Z. Weizhe, ``Blockchain-enabled decentralized trust management and secure usage control of IoT big data," IEEE Internet Things J., vol. 7, no. 5, pp. 4000_4015, May 2019

[11] Design and Implementation of an E-Policing System to Report Crimes in Nigeria. 10.1007/978-981-13-6351-1 21.

[12] Mollah, Muhammad Islam, Sikder Aman Ullah, Engr. Mohammad. (2012). Proposed e-police system for enhancement of e-government services of Bangladesh. 881-886. 10.1109/ICIEV.2012.6317444.

[13] P. Kormpho, P. Liawsomboon, N. Phongoen and S. Pongpaichet, ”Smart Complaint Management System,” 2018 Seventh ICT International Student Project Conference (ICT-ISPC), Nakhonpathom, 2018, pp. 1-6, doi: 10.1109/ICT-ISPC.2018.85239

[14] Mollah, Muhammad Baqer Islam, Kazi Islam, Sikder. (2012). EPolice System for Improved EGovernment Services of Developing Countries. Canadian Conference on Electrical and Computer Engineering. 10.1109/CCECE.2012.6335057.

[15] Onuiri, Ernest Oludele, Awodele A, Olaore O, Sowunmi A., UgoEzeaba. (2015). A REAL-TIME CRIME RECORDS MANAGEMENT SYSTEM FOR NATIONAL SECURITY AGENCIES. European Journal of Computer Science and Information Technology.

[16] Tasnim, Maisha Omar, Abdullah Rahman, Shahriar Bhuiyan, Md. (2018). CRAB: Blockchain Based Criminal Record Management System. 294-303. 10.1007/978-3-030-05345-1 25.