

Cryptoshield Fir System Using Blockchain Technology

Jayashri Mankar¹, Devesh Dhone², Prajkta Elinje³, Anushka Chaudhari⁴, Susmita Soma⁵

Genba Sopanrao Moze College of Engineering Balewadi, Pune-411045, Maharashtra, India.

ABSTRACT

Blockchain technology is a promising solution for managing electronic First Information Reports (e-FIR) in India, a country with a rising crime rate. The current centralized system poses significant risks, including hacking and fake reports, which compromise data transparency and integrity. To address these challenges, a consensus-based distributed blockchain solution using Ethereum blockchain technology is proposed, leveraging smart contract-based intelligent architecture to enhance data integrity and security. In India, traditional e-FIR databases are prone to tampering due to their centralized nature, allowing intentional false reports to be registered. Integrating e-FIR with a decentralized blockchain system can enhance data transparency and integrity by providing advanced security through encrypted blocks, utilizing Proof of Stake (PoS) protocol. This integration ensures transparency and strengthens data integrity in FIR registration processes. Blockchain technology offers a decentralized, secure, and transparent solution for managing FIR data, with smart contracts automating registration and access processes and cryptography for encryption before storage. This decentralized blockchain-based solution addresses the issue of handwritten FIRs and provides a secure storage solution for police-filed FIRs.

Keywords-Blockchain Technology, FIR, Security, Transparency, Decentralize.

INTRODUCTION

Smart cities rely on Information and Communication Technologies (ICT) to improve citizens' quality of life, promote sustainable growth, and ensure efficient governance. Major corporations like Intel, IBM, and Siemens are investing in futuristic smart city projects, driven by the rapid pace of urbanization. In a smart city, there is a need for a secure system for managing Electronic First Information Reports (e-FIRs) in police stations. E-FIRs are digital documents filed by victims or their representatives for cognizable offenses like murder, abduction, rape, or theft. However, challenges related to e-FIRs include non-registration, false enrolment, and data integrity issues stemming from police corruption, inefficiency, and lack of accountability. Blockchain technology can address these challenges by enhancing security and ensuring data integrity. Blockchain, known for its fraud-resistant, distributed ledger system, records transactions in a peer-to-peer network, providing decentralized and secure communication. This paper proposes a blockchain-enabled framework to ensure the integrity of e FIR data within smart city environments and minimize false enrolment of e-FIRs through blockchain technology. The Indian judicial system plays a pivotal role in ensuring the smooth functioning of the world's largest democracy. Effective record keeping within the police force is essential for maintaining an unaltered chronological sequence of events and documents. Traditional and current digital record-keeping systems often lack security and are susceptible to tampering. A blockchain based system offers a secure solution for record-keeping, ensuring data integrity and transparency in handling records. By integrating blockchain with IoT and Machine Learning, the system can be further strengthened, providing a robust framework for managing sensitive police records effectively.

Blockchain technology has emerged as a promising solution for E-FIR data management, enhancing security and efficiency in police investigations. By integrating blockchain into E-FIR data management, prevalent security challenges can be effectively mitigated. Blockchain's decentralized architecture revolutionizes data security and integrity by acting as a transparent and immutable ledger, ensuring the unalterable nature of each transaction. This eliminates concerns regarding non-registration, false registration, and data integrity breaches. The peer-to-peer network structure enhances E-FIR data efficiency and accessibility, fostering collaboration and coordination among law enforcement agencies.



Leveraging blockchain empowers smart cities to fortify crime management capabilities, ensuring a safer environment for citizens. FIR data management is a fundamental responsibility for law enforcement agencies globally, as it contains vital details such as the victim's and accused party's names, type and location of the crime, and other pertinent information crucial for investigations and judicial processes. In India, complaints concerning offenses must be registered under the law, which classifies offenses into cognizable and non-cognizable. The First Information Report (FIR) is filed at the police station in the event of a cognizable offense, detailing the complainant's information, incident's specifics, and other relevant details. Non cognizable offenses require obtaining a warrant from the court or magistrate before police intervention.

Blockchain technology, a decentralized network, is transforming the handling of police complaints, particularly First Investigation Reports (FIRs), by providing a robust framework for managing complaint records. Each node in the distributed fabric network, known as a zone, holds a copy of the blockchain, and when a new complaint is submitted, a timestamped FIR is generated and associated with the complaint, authenticated using a cryptographically produced hash key. This validation process, along with the timestamped FIR, is broadcasted to all nodes in the network. Efficient management of police complaints is crucial for upholding justice and order within society. In India, the process of registering complaints, particularly First Information Reports (FIRs), serves as a crucial step in initiating investigations and ensuring the prosecution of offenders. However, the existing complaint management system grapples with numerous challenges, including corruption, delays, and a lack of transparency. To address these hurdles, this paper advocates for the adoption of a blockchain-based police complaint management system.

METHODOLOGY

The police judicial record-keeping system is a critical component of the criminal justice system, and blockchain technology has emerged as a promising solution to this challenge. However, current systems often lack the ability to evolve into more intelligent platforms that can assist officers in making better and faster decisions. Integrating blockchain with emerging technologies like Machine Learning (ML), Internet of Things (IoT), and Artificial Intelligence (AI) can enhance the system's capabilities.

ML enables computers to learn from data and discover hidden patterns or insights, improving workflow and optimizing time efficiencies. It can prioritize cases, suggest the likelihood of a complaint being genuine, or determine if it constitutes a cognizable offense. Furthermore, extending the scope of the blockchain framework with additional functionalities such as secure logistics management for evidence transportation and criminal relocation can further enhance the system's utility. Creating a blockchain-based ecosystem for managing police stations and jails could involve additional tracking functionalities, such as monitoring jail visitors or tracking the behavioural progress of incarcerated individuals. Smart contracts can automatically log complaints initiated by citizens, ensuring no First Information Reports (FIR) goes unrecorded. ML can improve accessibility by providing features such as text-to-speech for FIR and update read-outs for the visually impaired. The Internet of Things (IoT) can leverage sensors and devices to capture information related to criminal cases, enabling secure storage and access of evidence and case-related information by police officers. ML algorithms can analyse data collected from these devices to derive insights and aid in decision-making processes.

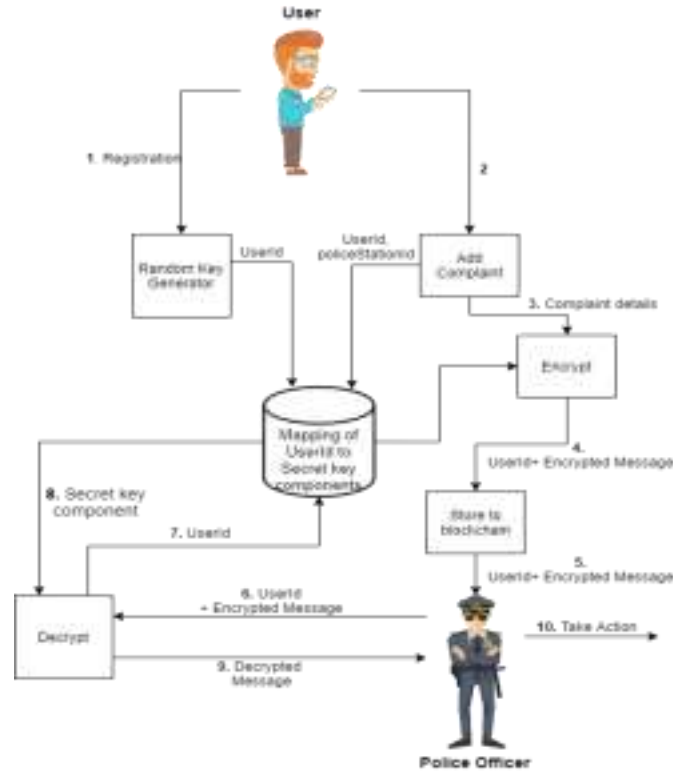


Figure 1 Security Module

• Implementation:

The e-FIR (First Information Report) system is a blockchain-based system that integrates three core modules: User, Police Officer, and Admin. It uses various technical specifications such as the Third web platform, Matic currency, JavaScript, Next.JS, Express.JS, and smart contracts using Solidity. Users can submit complaints securely stored on the blockchain network, while the Police Officer module allows authorized personnel to view, investigate, and update the status of FIRs. Smart contracts, coded in Solidity, define and enforce the business logic of the e-FIR system, ensuring secure and trustless interactions.

The admin module manages the e-FIR system, verifying each transaction. JavaScript, Next.JS, and Express.JS are used for the development of both the user interface and backend services. These technologies facilitate efficient development and deliver a seamless user experience within the e-FIR system. During the implementation phase, careful planning and investigation of system constraints are crucial for translating the design into a functional system. Key tasks include careful planning, thorough investigation of the system and its constraints, designing methods for transition from design to implementation, evaluating chosen implementation methods, and making correct decisions regarding the platform selection.

The front-end of the system is developed using ASP.NET, which allows for the isolation of code and HTML, facilitating efficient development and maintenance. SQL Server is used on the backend for storing data across multiple instances, offering scalability suitable for handling diverse data storage requirements within the project.

The implementation of the system involves several steps on both the user and police sides:



- d. File Download: Officers download files using their private keys for secure access.
- e. Access Control Verification: The system verifies access control settings before file download to ensure authorized access. This implementation ensures a secure and efficient process for users to register complaints and for police officers to access and download relevant files based on assigned privileges and access control settings.

RESULT & DISCUSSION

The central outline of the proposed algorithm is the implementation of health care data storage using block chain. System creates the trustworthy communication between multiple parties without using any third-party interface. We use the Hash generation algorithm and the Hash will be generated for the given string. Before executing any transaction, we use peer to peer verification to validate the data .

Tools and Technologies Used

Software Interfaces:

The Interface will be in the form of an application. It is designed to be functional and minimal in its styling. All options will be displayed in a menu based format. Web application will be used to setup the page layout and add minimal styling to make the interface user friendly.

- Operating system: OS.
- Coding Language : Java
- Database :MYSQL
- IDE : Eclipse IDE
- Front End: JSP and Servlet
- Back End Servlet/Data Base(MYSQL)

Hardware Interfaces

A webserver will be required so that the students and the mess admin can connect to it to exchange information. The servers have a database to store all the data entries. The Server will have to have a high speed 1 Gigabit Ethernet connection to the college's local network.

- Processor:- Intel Pentium 4 or above
- Memory:- 2 GB or above
- Other peripheral:- Printer
- Hard Disk:- 500gb

Pseudo Code

Algorithms 1: SHA-256 Values Generation

Input: The original block, previous-hash, and data d,

Output: The hash H was generated based on the provided data's.

Step-1: The record is inputted as d.

Step-2: Utilize SHA-256 from the hash values range.

Step-3: C_Hash= SHA-256(d)

Step-4: Retrun C_Hash

Algorithms 2: Peer-to-peer (P2P) verification protocols

Input: The user receives an IP address and a User Transaction TID.

Output: Activate the IP address or current query to determine the validity of any connection.

Step 1: The user generates a mysql query using DDL, DML, or DCL.

Step 2: Retrieve the present IP address.

For each (read IP into IP address)

```

If(Assuming that the connection (IP) is true)
Flag=true
Else
Flag=false
End for-each
Step 4 : if (Flag.equals(valid))
Peer-to-peer (P2P) verification valid
Else
Peer-to-peer (P2P) verification Invalid
End if
End for
  
```

Algorithms 3: Mining Algorithm for valid hash creation

Input: Hash Validation Policy P[], Current Hash Values hash_Val
Output: Valid hash
Step 1: System generate the hash_Val for ith transaction using Algorithm 1
Step 2: if (hash_Val.valid with P[])
 Valid hash
 Flag =1
Else
 Flag=0
 Mine again randomly
Step 3: Return valid hash when flag=1

Algorithms (Encryption and Decryption) PBEWithMD5AndDES

KeyGen (M) ->K is the key generation algorithm that maps a data copy M to a convergent key K. Enc (K, M) -> C is the PBEWithMD5AndDES encryption algorithm that takes both the convergent key K and the data copy M as inputs and then outputs a cipher text C;

Dec (K, C) ->M is the decryption algorithm that takes both the cipher text C and the convergent key K as input and then outputs the original data copy M

Screenshots:



CONCLUSION

The Indian Police Services handle over 50 lakh complaints annually, but they still face challenges in processing handwritten reports and handling sensitive data. A proposed system aims to address these issues by providing a secure and transparent platform that safeguards data confidentiality while ensuring transparency in the complaint handling process. This system encourages individuals to report incidents, knowing that their complaints will be taken seriously by the police. It also streamlines the cumbersome process of filing reports, such as First Information Reports (FIRs), for police officers, improving overall efficiency.

A comprehensive study of Indian police case record management systems revealed the need for a modern, unalterable, transparent, accountable, traceable, and chronological system to enhance efficiency and mitigate malpractices in the case management process. Blockchain technology was identified as an ideal fit for addressing these challenges, and various blockchain-based systems were reviewed to evaluate their advantages and drawbacks. However, India is still in the process of developing the necessary infrastructure for a blockchain-based online system, including storage capabilities, widespread accessibility, online facilities, and a skilled and trustworthy human resource pool.

Blended police record management system solutions are proposed as a potent alternative to achieve an efficient, tamper proof case management system. These solutions integrate elements from traditional and modern approaches to provide a robust framework for managing police cases effectively. The project aims to bolster the security, transparency, and efficiency of the e-FIR (Electronic First Information Report) process through the utilization of blockchain technology. The envisioned outcomes include increased data security, amplified transparency, streamlined processes, and enhanced trust within the e FIR ecosystem. The proposed blockchain-based First Information Report (FIR) data management system offers a secure, decentralized, and transparent solution to address issues such as data tampering, unauthorized access, and lack of transparency. By leveraging blockchain technology, the system ensures data integrity, confidentiality, and authenticity while providing transparency and accountability to all stakeholders involved. This enhanced framework has the potential to enhance the efficiency and effectiveness of FIR data management, empowering law enforcement agencies to uphold law and order more effectively. The proposed system aims to streamline the FIR process while ensuring its protection.

REFERENCES

- [1]. Li, T., Li, D., & Wang, M. "Blockchain-based fair and decentralized data trading model." *The Computer Journal*, 65(8), 2133-2145, Aug. 2021.
- [2]. Li, T., Ren, W., & Xiang, Y. "FAPS: A fair, autonomous, and privacy-preserving scheme for big data exchange based on oblivious transfer, ether cheque, and smart contracts." *Information Sciences*, 544, 469-484, Feb. 2021.
- [3]. Lin, Chao, Debiao He, Xinyi Huang, and Kim-Kwang Raymond Choo. "OBFP: Optimized blockchain-based fair payment for outsourcing computations in cloud computing." *IEEE Transactions on Information Forensics and Security* 16 (2021): 3241-3253.
- [4]. Xiong, W., & Xiong, L. "Anti-collusion data auction mechanism based on smart contract." *Information Sciences*, 555, 386-409, May 2021.
- [5]. 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.
- [6]. Zhaofeng, M., Lingyun, W., Xiaochang, W., Zhen, W., & Weizhe, Z. "Blockchain-enabled decentralized trust management and secure usage control of IoT big data." *IEEE Internet Things Journal*, 7(5), 4000-4015, May 2019.
- [7]. Gupta, Antra, & Vilchez Jose, D. "A Method to Secure FIR System using Blockchain." *International Journal of Recent Technology and Engineering (IJRTE)*, ISSN: 2277-3878, Volume-8, Issue-1, May 2019.
- [8]. Tabassum, K., Shaiba, H., Shamrani, S., & Otaibi, S. "e-Cops: An Online Crime Reporting and Management System for Riyadh City." 2018 1st International Conference on Computer Applications Information Security (ICCAIS), Riyadh, 2018, pp. 1-8. doi: 10.1109/CAIS.2018.8441987.
- [9]. Iyer, A., Kathale, P., Gathoo, S., & Surpam, N. "E-Police System-FIR Registration and Tracking through Android Application." *International Research Journal of Engineering and Technology*, 3(2), 1176-1179, 2016.
- [10]. Pillai, P. A. K. S. Y. K. S. "Online FIR Registration and SOS System." *International Journal of Engineering, Computer, and Science*, vol. 5, no. 4, Dec. 2017.
- [11]. Misra, Sanjay, Maskeliunas, Rytis, & Damaševičius, Robertas. "Design and Implementation of an E-Policing System to Report Crimes in Nigeria." 10.1007/978-981-13-6351-1 21, 2019.



- [12]. Mollah, Muhammad Islam, Sikder Aman Ullah, & Engr. Mohammad. "Proposed e-police system for enhancement of e government services of Bangladesh." Canadian Conference on Electrical and Computer Engineering. 10.1109/ICIEV.2012.6317444, 2012.
- [13]. Kormpho, P., Liawsomboon, P., Phongoen, N., & Pongpaichet, S. "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. "E-Police System for Improved E-Government Services of Developing Countries." Canadian Conference on Electrical and Computer Engineering. 10.1109/CCECE.2012.6335057, 2012.