International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 5 ǁ May 2023 ǁ PP. 31-36

Smart FIR: Securing e-FIR Data through Blockchain

Yash Falke[1], Harsh Sunwani[2], Nikhil Jaiswal[3], Siddhesh Wani[4],
Ichhanshu Jaiswal[5]

[*1234] *BE Undergraduate Vidyalankar Institute of Technology, University of Mumbai, India*
[*5] *Assistant Professor, Undergraduate Vidyalankar Institute of Technology, University of Mumbai, India*

Abstract

When a cognizable offence like murder, abduction, rape, theft, etc. is committed, a victim or someone acting on their behalf must submit an electronic first information report (e-FIR) to the police station. Due to the centralized nature of the e-FIR database, it is possible for the offense's record to be hacked, and it is also possible for fake e-FIRs to be purposefully registered. Data transparency and integrity are therefore major issues with the e-FIR database. In this study, a consensus-based distributed blockchain approach is used to solve e-FIR data integrity and false registration added with police stations in a centralized database as a crucial component of a smart city environment. Specifically, the potential of the Ethereum blockchain in delivering integrity has been investigated using a smart contract-based intelligent architecture.

Keywords: *e-FIR, Smart cities, Smart contract, Blockchain, Data integrity*

Date of Submission: 19-04-2023 Date of acceptance: 03-05-2023

I. INTRODUCTION

Smart Metropolises explosively calculate on the conception of Information and Communication Technologies (ICT), which invest in human social life to ameliorate their citizens quality of life, by stimulating profitable growth, sustainable good governance, wise coffers operation, and effective mobility, whilst they guarantee the security and sequestration of their citizens [1]. Giant companies like Intel, IBM and Siemens are monstrously investing in futuristic smart metropolises [2], as the rearmost statistics show that urbanization is progressing at an unknown pace. According to the UN report of 2018, presently, further than percent of the World's population lives in metropolitan metropolises and is anticipated to grow up to 66 percent by 2050 [3]. also, smart megacity structure needs effectiveness in numerous aspects, from resource allocation to energy consumption, social security to health operation [4], and safe megacity [5] to the felonious record operation system.

In a smart megacity of smart vehicles, smart seminaries, smart hospitals, smart structure etc., where everything is connected to the Internet(IoE) [6] to partake tremendous data volume daily, this megacity should also give a smart and secure system for Electronic First Information Report(e-FIR) data operation in a police station as shown in Fig. 1. e-FIR is a simple document that has been written out and filed to the police by the victim or someone on his/ her behalf when a cognizable suitable offense similar as murder, hijacking , rape, theft, etc. is married. Reporting a crime and filing a cognizable offense manually in a police station consumes a lot of time because the police to people rate in some of the state countries are extensively high as shown in Table 1. rather, the e-FIR medium is used in some of the state countries i.e. Pakistan, India, Bangladesh, Malaysia, Japan and Singapore, while the medium for filing an offense in Europe and USA is, supposedly, different than the forenamed countries [7].

Non-registration, false enrolment and integrity of e-FIR data are the main concerned problems connected with it. These problems are due to police corruption, inefficiency and warrant of responsibility. Originally, e-FIR data is stored in a central database of police station locally, which is also participated with the headquarter(HQ) of police stations. Then the e-FIR data could fluently be manipulated as the control of e-FIR database is original within the police station. thus, to address this problem, applying blockchain technology can help us to more respond to the security challenges and can endeavour data integrity, as blockchain is a fraud-flexible, distributed tally, which can record all the deals in a Peer-to-Peer(P2P) network. Blockchain has a decentralized armature, and its fashion ability in the cryptocurrency world in securing the distributed network communication has been remarkable [8]

In this paper, the major benefactions are twofold originally, a blockchain- enabled frame furnishing effective integrity to e-FIR data is proposed, which is applicable in, and been an integrated part of, a smart megacity terrain. Secondly, false enrolment of e-FIR is minimized by resolving it through the conception of blockchain. To the stylish of our knowledge, this is a first attempt restraining false enrolment and furnishing integrity to e-FIR data using blockchain.

No.	Country	People-Police Ratio
1	Bangladesh	1:1138
2	India	1:728
3	Pakistan	1:625
4	Singapore	1:614
5	Malaysia	1:450

Table I: POLICE TO PEOPLE RATIO IN SOME COUNTRIES [19]

II. E-FIR BACKGROUND AND RELATED WORK

In colorful systems, felonious records and different offenses data are generally stored in centralized storehouse. Still, there can be multiple scarcities in centralized systems, similar as single point of failure. On the other hand, different offenses data stored in original database in a police station are largely vulnerable to the following issues:

- **Data Tampering**: Storing data in a local database of an institution can allow the superior authority to manipulate the crucial data without taking any other authority into consideration. The only way to solve this issue is to mark every single data with digital signature and distribute it among different entities to keep the data transparent.
- **False Registration**: Police officials having access to data stored in local database can register false case on anyone without disclosing the personal identification number (ID) and credentials of the officer in-charge (admin) with the case. To identify the right person being involved in the false case is a challenge, and it can only be handled by sharing the admin credentials with different entities, so it could be used for auditing purpose.

In order to ameliorate system security and give integrity to the offenses data, a decentralized consensus-based approach is needed, where the user can trust the system to interact and share information without being concerned about data tampering.

Blockchain has recently gained prominent popularity, mostly due to its distributive nature, where the blockchain decouples the centralized hold from single entity and gives control to multiple participating entities, who validate the authenticity of the records and make the ledger completely transparent. There are two main types of networks in blockchain, that is, public and private network blockchain. Bitcoin [9] and Ethereum refers to public blockchain using Proof-of-Work (PoW) concept, and Hyperledger-fabric refers to private blockchain using Proof-of-Authority (PoA) concept, where all operate in a trust less environment for online P2P transactions. The most hyped alternative created for the cryptocurrency application is the smart contract paradigm, where Ethereum and Bitcoin were deployed and served as cryptocurrencies [10], [11]. A smart contract is a software-defined protocol that can digitally verify, facilitate or even enforce the negotiations of a contract. Smart contracts execute intelligent transactions without any third party's intervention and those transactions are traceable and irreversible [12]. Ethereum is one of the blockchain platforms, which allows us to interact with object-oriented solidity programming for writing smart contracts.

Researchers have opted Blockchain for many diverse problems. Antra et al. [13] have discussed an idea of how to secure online FIR with blockchain by registering the complainer, suspect and witness to the system interface. In this work, the pre-registration of the process is conducted by the officer in charge and the user credentials are stored in a local database, which can result in non-registration of FIR by making changes to the user authentication data. The authors also lacked in not addressing the issue of false FIR handling. Maisha et al. [14] have proposed a blockchain-based system for securing merely the criminal data into the blockchain distributed ledger and restraining the data from any unlawful changes by unauthorized personnel. A technique of pre-registering users to the system has been used and the criminal data is uploaded to the cloud repository. The authors lacked in addressing the integrity of user's data stored on cloud database, which eventually does not consider the case of false FIR registration. Kirti et al. [15] have proposed a portal-based e-FIR system, in which an administrator ensures the authenticity and integrity of the FIR data by only filing the pre-registered FIR in the local database, which provides transparency using e-governance. However, the authors lacked in addressing the data integrity even if they use the pre-registering technique. Muhammad Baqer Mollah et al. [16] have introduced a system in which, the home ministry would be connected with all the police stations in a city in Bangladesh, called the 'Third Eye', and its sole purpose would be to keep track on police stations activities and records. Here, home ministry officials have access to the data and could be tampered easily due to the existence of a central database, which is solely managed by the home ministry officials.

According to the literature review, no previous work has a focus on providing intelligent integrity to e-FIR data and handling false registration of e-FIR stored in central database in a police station. For this issue, we propose a consensus based blockchain framework, where multiple participating entities are involved to maintain the transparency of e-FIR data.

III. PROPOSED BLOCKCHAIN-BASED FRAMEWORK

By addressing an important challenge—namely, how intelligent integrity could be provided to e-FIR data stored in the centralized database of a police station in a fully connected digital city (smart city) interoperability scenario—the proposed intelligent framework makes use of the benefits of the blockchain technology. The goal is to provide transparency by decentralizing the authorities' control over the e-FIR data stored in a police station's central database among various entities. The novel framework that is specifically proposed in this paper has two components:

- A tamper-proof and fraud-resistant intelligent system that uses distributed blockchain ledgers and smart contracts is proposed to provide e-FIR data integrity.
- The credentials of both the user and the admin are gathered and stored on the blockchain for auditing purposes in order to combat false e-FIR registration.

2.1. System Architecture

We assume that the identification information of citizens kept in a nation's national database is safe and secure and that the system interface (SI), from which a user can register for an e-FIR, is linked to the national database for user authentication. The proposed system architecture's workflow, as depicted in Fig. 2, is briefly explained as follows:

i. **Registration of Police Stations:** Using a smart contract, the superintendent of police (SP) at the headquarters creates a distinct account address for each and every police station, known as the police station's hash, which is then stored or registered on the blockchain ledger. In PoW, all participating addresses start the mining process in a consensus and the block is mined for the address that successfully solves the challenging puzzle. In contrast, the authority address in PoA is only accountable for mining the blocks. The following information is integrated into each police station's hash and is used for auditing purposes.
   - City and location of the police station.
   - In-charge (admin) of the police station.
   - Names of all the investigating officers

   The administrator of that specific police station is responsible for informing the HQ when a new investigating officer is appointed. This allows the HQ staff to update the police station's credentials and create a new blockchain transaction. The new appointment will be made known to all participating addresses (police stations). The administrators of the police stations would also follow the same process.

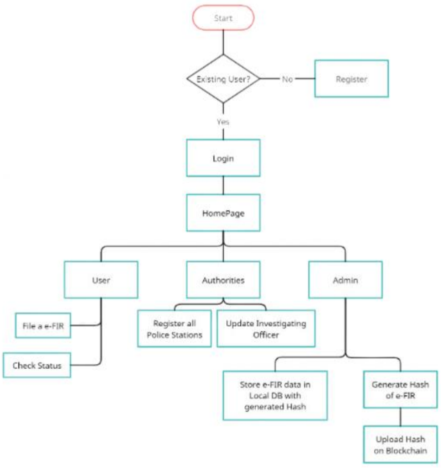
Start
Existing User?
No
Register
Yes
Login
HomePage
User
Authorities
Admin
File a e-FIR
Check Status
Register all Police Stations
Update Investigating Officer
Store e-FIR data in Local DB with generated Hash
Generate Hash of e-FIR
Upload Hash on Blockchain

Figure 1: Flow diagram of the proposed blockchain-based architecture.

ii. **User Filing an e-FIR:** The user interacts with the SI by entering an ID for validation, which is carried out at runtime from the citizen's national database because it is linked to the SI, and only permits them to file an e-FIR in the event of cognizable offences. The user will not be permitted to modify the e-FIR if it has already been submitted and is still pending because doing so would change the original hash value, which would indicate changes to the original e-FIR data and aid in the detection of fraud. When submitting an e-FIR, the user must include the following information (plus any additional data, if any).

- Time, date and place of the offence and the reporting.
- All personal details of the complainant and accused.
- Complete detailed description of the offense.
- Any additional evidence for proof (if any).
- Description of the property stolen (if any).
- Police station where the offense is registered.

iii. **Admin Approves e-FIR Transaction:** The admin is in charge of approving all blockchain transactions. When a user submits an e-FIR, the administrator of the police station designates one of the investigating officers to investigate the case and verify the information submitted by the user. If the data is confirmed to be accurate, the admin creates a hash of that e-FIR data and uploads it using a smart contract to the distributed private blockchain. Additionally, the user-provided e-FIR details are digitally signed with the precise hash generated for that e-FIR data before being uploaded to the police station central database. The hash will serve as the e-FIR's ID. If fraudulent e-FIR data is discovered, the admin will not approve the transaction and hence, the case and the transaction will be dropped.

iv. **Dealing with False e-FIRs:** If the police administrator or user station tries to falsely file an e-FIR against someone on purpose, the accused user will have the right to request an auditing of erroneous e-FIR from the SP. The SP has access to the hash data as well as all other case information, including the city and police station, the police station administrator, the investigating officer, and the data from the e-FIR that was purportedly filed against the accused user. They are unable to remove their identities from the blockchain ledger to erase the evidence that they were not involved in the case because the credentials of all parties involved who have allegedly filed e-FIRs are saved on the blockchain in the form of hashes. Blockchain also keeps track of timestamp of every block transaction, which can further aid in identifying the involvement of a person in fraudulence.

IV. IMPLEMENTATION

2.2. User Interface

We are using the MERN (MongoDB, ExpressJs, ReactJs, NodeJs) stack, which will directly connect to the Ethereum blockchain. With this setup, the ReactJS interface will allow users to input data, which will be stored in MongoDB. NodeJs will be used to create an API that enables communication between the MongoDB backend and the ExpressJs framework, which will handle incoming requests from the frontend. Web3 provider like Meta Mask are used to connect to the Ethereum blockchain. The smart contract for the system can still be developed using the Remix IDE and deployed on a Web3 RPC environment. When new data is added to MongoDB, it can be directly sent to the blockchain via the Web3 provider, where it will be stored as a transaction on the Ethereum network. This creates an immutable and transparent record of the data.

2.3. Ethereum Blockchain

We used the Ethereum blockchain's Ganache software, a development tool made available by Ethereum developers. The advantage of using Ganache is that it offers 10 different accounts, each with 100 ethers, and those ethers can be used only for development. Building and implementing a personal blockchain that allows us to create multiple unique addresses for each node is necessary for the system's scalability. The advantage of personal blockchain is that, if we designate an authority to handle block mining, the mining process becomes very quick since the authority is only tasked with using computing power to handle block mining. Ethereum uses the PoW concept for mining; however, PoA benefits may be obtained by defining functions in a smart contract and allocating specific addresses to particular operations. For example, in our model, we gave some addresses the power to carry out certain tasks that other addresses are unable to, such as registering all police stations from the SP node address and approving e-FIR transactions from the admin node address.

2.4. Smart Contract

In our model, we created a smart contract that receives data in the form of hashes and stores it on the blockchain using the Solidity programming language in the Remix IDE for the Ethereum blockchain. The following functionalities are included in smart contracts, as discussed in Section III.

- Registering all Police Stations.
- Uploading Hash on Blockchain.
- Updating Investigating Officer

We have used a variety of hashing algorithms in the implementation of the blockchain-based framework. In the Ethereum ecosystem, "gas" is a unique unit that measures the amount of computational work required to complete a given operation. The most sophisticated and secure hashing algorithm is SHA-512 (512 bits), but it uses more gas, reducing the number of transactions per blockchain block. However, using SHA-1 (160 bits) will allow us to fit more transactions into a single block, but the hashing security will be lower because SHA-1 is less secure than SHA-512. Therefore, using SHA-256 (256 bits) could attempt data integrity by having a sufficient hashing security level while using a moderate Gas value.

2.5. System Specifications

We have tested the proposed e-FIR model on the following system specifications, as shown in Table II.

System RAM	8 GB DDR4
Hard Drive	128 SSD/640 HDD
System Core	Intel Core i5
Operating System	Windows 10

Table II: SYSTEM SPECIFICATIONS

V. METHODOLOGY

Agile practices have been applied in the development of nonreal-time critical blockchain-based software. These practices, such as active user involvement, short cycles, and iterative releases, are commonly used in agile software development methodologies like SCRUM and XP. Agile prototyping, or Spike Solution in XP, has been found to be particularly useful at the early stages of blockchain-based software development. It helps with requirements elicitation, specification, and identifying uncertainties in system quality factors such as transaction execution performance and security. However, smart contracts are immutable after deployment on distributed ledgers, and access by external users is strictly forbidden due to the security model defined by blockchain architecture. Therefore, agile practices may not always be suitable for developing ever-changing business services, and software teams should implement smart contracts for business services with minimum upgrade needs at runtime and ensure their verification before deployment on blockchain platforms. The steps we will be following in iteration are as below:

- Define
- Design
- Build
- Test
- Release
- Review

VI. CONCLUSION

This study investigates the use of blockchain technology to address the issue of data tampering and false report filing in police stations, which is a relatively under-developed area of record management. The paper proposes a consensus-based solution to ensure data integrity for offenses stored in police station databases using blockchain. The proposed framework interfaces React.js with Ethereum blockchain using Nodejs and MongoDB, enabling secure e-FIR data transactions via smart contracts. Various simulations were conducted to illustrate the trade-off between the number of transactions occurring in a single block and the level of hashing security for e-FIR data.

VII. FUTURE WORK

In the future, the proposed system will be examined for its ability to dynamically choose different hashing algorithms according to the classification and significance of the offenses data. Additionally, the system will optimize Gas value utilization in Ethereum blockchain by identifying the data type and importance of the offense, thereby maximizing the number of transactions stored in a single block.

ACKNOWLDGEMENTS

We would like to express our sincere appreciation and gratitude to our project guide, Prof. Ichhanshu Jaiswal, for his tremendous support and guidance. Without his guidance, our project would not have been possible. We also extend our thanks to Dr. Vipul Dalal, the Head of the Department of Information Technology, for providing valuable advice throughout the project. We are grateful to all the staff members who willingly assisted us. Lastly, we would like to thank Vidyalankar Institute of Technology for granting us this opportunity.

REFERENCES

[1]. P. A. Perez-Martinez et al. “Privacy in Smart Cities- A Case Study of Smart Public Parking,” Proc. 3rd Int’l Conf. Pervasive Embedded Computing and Commun. Sys., pp.55–59, 2013.

[2]. M. Dohler et al., Eds., “Feature Topic on Smart Cities”, IEEE Commun. Mag., vol, 51, no. 6, 2013.

[3]. [Online: January, 2019] Urban Population Growth statistics by UN; https://population.un.org/wup/Publications/Files/ WUP2018-Report.pdf

[4]. Agusti Solanas et al., “Smart Health: A Context-Aware Health Paradigm within Smart Cities”, IEEE Commun. Mag., vol, 52, no. 8, 2014.

[5]. Jaime Ballesteros et al. “Safe Cities. A Participatory Sensing Approach”, IEEE LCN, 2012.

[6]. Paola G. V. et al., ”FOCAN: A Fog-supported Smart City Network Architecture for Management of Applications in the Internet of Everything Environments”, J. Parallel Distrib. Comput., 2018.

[7]. [Online: March, 2019] Website of US department of justice for reporting a crime; https://www.justice.gov/actioncenter/report-crime.

[8]. R. M. Parizi et al., “Empirical vulnerability analysis of automated smart contracts security testing on blockchains” CASCON, IBM Corp., 2018.

[9]. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” white paper, 2008.

[10]. T. T. A. Dinh et al., ”Un-tangling Blockchain: A Data Processing View of Blockchain Systems,”in IEEE Transactions on Knowledge and Data Engineering, vol. 30, no.7, pp. 1366-1385, 1 July, 2018.

[11]. Jean Bacon et al., ”Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralized Ledgers”, 25 RICH. J.L. and TECH., no. 1, 2018.

[12]. Reyna et al., ”On blockchain and its integration with IoT. Challenges and opportunities.” Future Generation Computer Systems, vol 88, 2018.

[13]. Antra Gupta et al., “A Method to Secure FIR System using Blockchain”, IJRTE, Vol. 8, Issue-1, 2019.

[14]. Maisha A. Tasnim et al., “CRAB: Blockchain Based Criminal Record Management System”, SpaCCS, LNCS 11342, pp. 294–303, 2018.

[15]. Kirti Marmat et al., “E-FIR using E-Governance”, IJIRST, vol. 3, 2016.

[16]. Muhammad Baqer Mollah et al., “Proposed E-Police System for Enhancement of E-Govemment Services of Bangladesh”, IEEE/OSA/IAPR, 2012.

[17]. [Online: January, 2017] Personal blockchain for Ethereum development;
https://www.trufflesuite.com/docs/ganache/overview.

[18]. [Online: November, 2019] Josh Cassidy, Article for Online Remix IDE- writing smart contract; https://kauri.io/remix-ide-your-first-smart-contract/124b7db1d0cf4f47b414f8b13c9d66e2/a.

[19]. [Online: October, 2011] Bangladesh Police’s Website, Police to People Ratio; http://www.police.gov.bd/index5.php?category=48.

[20]. A. B. Masood et al., ”Realizing an Implementation Platform for Closed Loop Cyber-Physical System using Blockchain”, IEEE 89th VTC, 2019.