Smart FIR: Securing e-FIR Data through Blockchain within Smart Cities

Nasir D. Khan, Chrysostomos Chrysostomou
Department of Electrical and Computer Engineering and Informatics, Frederick University.
Nicosia, Cyprus.
st017021@stud.frederick.ac.cy, ch.chrysostomou@frederick.ac.cy

Babar Nazir
Department of Computer Science, COMSATS University Islamabad.
Abbottabad, Pakistan.
babarnazir@cuiatd.edu.pk

***Abstract*—Electronic First Information Report (e-FIR) is a basic document filed to the police stations by a victim or someone on his/her behalf when a cognizable offense such as murder, kidnapping, rape, theft, etc. is committed. In the e-FIR database, the offense's record can be compromised due to its centralized nature, and further the intentional registration of false e-FIR can occur. Thus, data integrity and transparency are key concerns in e-FIR database. In this paper, e-FIR data integrity and false registration appended with police stations in a centralized database are addressed via a consensus-based distributed blockchain solution, as an integral part of a smart city environment. Specifically, a smart contract based intelligent framework has been utilized to explore the potential of Ethereum blockchain in providing integrity to e-FIR data stored in a police station's database. Local database is interfaced with Ethereum blockchain using Web3 Remote Procedure Call (RPC) protocol. Multiple simulations have been performed to evaluate the performance of the proposed framework. Our results show a trade-off between different hashing algorithm security level for the offenses data and number of transactions stored in a single block on blockchain ledger.**

***Index Terms*—e-FIR, Smart cities, Smart contract, Blockchain, Data integrity.**

I. Introduction

Smart cities strongly rely on the concept of Information and Communication Technologies (ICT), which invest in human social life to improve their citizens' quality of life, by stimulating economic growth, sustainable good governance, wise resources management, and efficient mobility, whilst they guarantee the security and privacy of their citizens [1]. Giant companies like Intel, IBM and Siemens are hugely investing in futuristic smart cities [2], as the latest statistics show that urbanization is progressing at an unprecedented pace. According to the UN report of 2018, currently, more than 50 percent of the World's population lives in metropolitan cities and is expected to grow up to 66 percent by 2050 [3]. Moreover, smart city infrastructure needs efficiency in many aspects, from resource allocation to energy consumption, social security to health management [4], and safe city [5] to the criminal record management system.

In a smart city of smart vehicles, smart schools, smart hospitals, smart infrastructure etc., where everything is connected to the Internet (IoE) [6] to share tremendous data volume daily, this city should also provide a smart and secure system for Electronic First Information Report (e-FIR) data management 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 offense such as murder, kidnapping, rape, theft, etc. is committed. Reporting a crime and filing a cognizable offense manually in a police station consumes a lot of time because the police to people ratio in some of the commonwealth countries are tremendously high as shown in Table I. Instead, the e-FIR mechanism is used in some of the commonwealth countries i.e. Pakistan, India, Bangladesh, Malaysia, Japan and Singapore, while the mechanism for filing an offense in Europe and USA is, apparently, different than the aforementioned countries [7].

Non-registration, false registration and integrity of e-FIR data are the main concerned problems connected with it. These problems are due to police corruption, inefficiency and lack of accountability. Initially, e-FIR data is stored in a central database of police station locally, which is then shared with the headquarter (HQ) of police stations. Here the e-FIR data could easily be manipulated as the control of e-FIR database is local within the police station. Therefore, to address this problem, applying blockchain technology can help us to better respond to the security challenges and can endeavour data integrity, as blockchain is a fraud-resilient, distributed ledger, which can record all the transactions in a Peer-to-Peer (P2P) network. Blockchain has a decentralized architecture, and its popularity in the cryptocurrency world in securing the distributed network communication has been remarkable [8].

In this paper, the major contributions are twofold: Firstly, a blockchain-enabled framework providing efficient integrity to e-FIR data is proposed, which is applicable in, and been an integrated part of, a smart city environment. Secondly, false registration of e-FIR is minimized by resolving it through the concept of blockchain. To the best of our knowledge, this is a first attempt restraining false registration and providing integrity to e-FIR data using blockchain.

The rest of paper is organized as follows. Section II discusses e-FIR and relevant approaches therein. Section III presents the proposed system architecture. The proposed framework implementation and evaluation results are shown in Section IV. Finally, the concluding remarks with future work is given in Section V.

978-1-7281-5207-3/20/$31.00 ©2020 IEEE

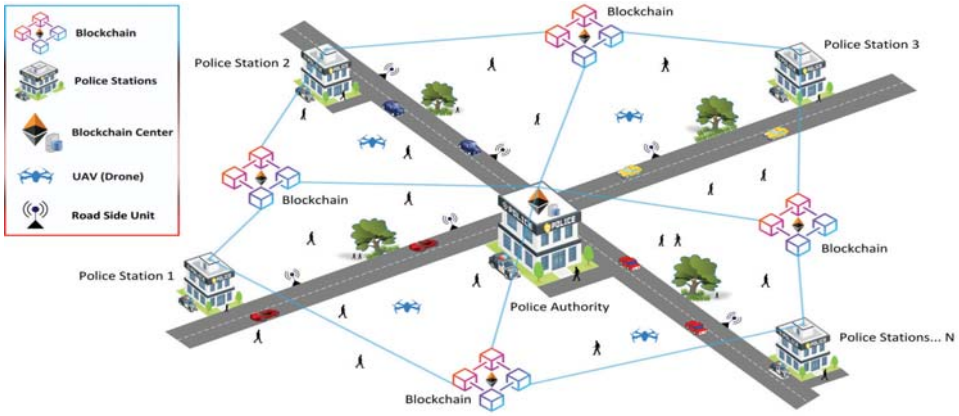

Fig. 1: System model of smart police stations in a smart city environment.

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

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

II. E-FIR Background And Related Work

In various systems, criminal records and different offenses data are usually stored in centralized storage. However, there can be multiple deficiencies in centralized systems, such as single point of failure. On the other hand, different offenses data stored in local database in a police station are highly 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 improve system security and provide integrity to the offenses data, a decentralized consensus-based approach is required, 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 trustless 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

The proposed intelligent framework utilizes benefits of the blockchain technology 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 vision is to decentralize the authorities hold on e-FIR data in a central database of police station among different entities to provide transparency. In this paper, the proposed novel framework is specifically twofold:

- An intelligent system is proposed to provide e-FIR data integrity through distributed blockchain ledger, using smart contract, which is tamper-proof and fraud resilient.
- False e-FIR registration is also dealt by collecting the credentials of both the user and the admin and storing them on the blockchain for auditing purpose.

A. System Architecture

We assume that the ID of citizens stored in a national database of a country are safe and secure, and the system interface (SI) from which e-FIR can be registered by the user, is connected with the national database for user authentication. The workflow of the proposed system architecture, as shown in Fig. 2, is briefly elaborated as follows:

1) **Registration of Police Station:** The superintendent of police (SP) in the HQ generates a unique account address for every single police station, called hash of the police station and it is stored/registered on the blockchain ledger using smart contract. In PoW, all the addresses initiate the mining process in a consensus and whichever participating address achieves in solving the complex puzzle, then its block is mined. On the other hand, in PoA, the authority address is only responsible for mining the blocks. In the hash of an individual police station, the following details are integrated with it, which are used for auditing purpose.

- City and location of the police station.
- In-charge (admin) of the police station.
- Names of all the investigating officers.

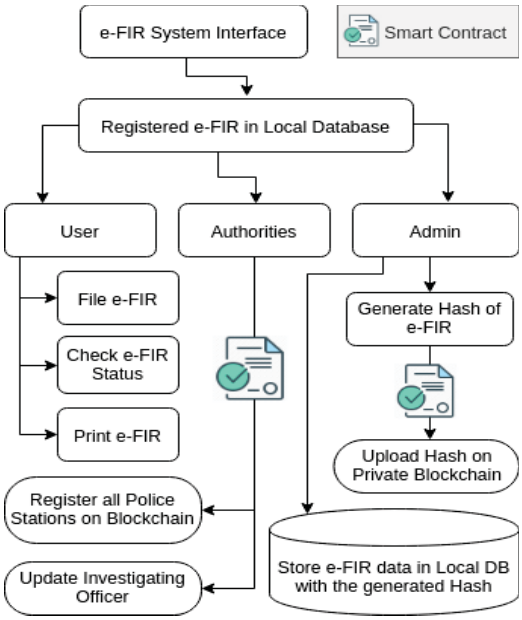

Fig. 2: Flow diagram of the proposed blockchain-based architecture.

In case of a new investigating officer selected in the police station, the admin of that particular police station would be liable to inform the HQ, so that the officials of HQ would update the credentials of that police station and make a new transaction on the blockchain. All the participating addresses (police stations) will also know about the new appointment. Likewise, the same procedure would also be followed for the admins of the police stations.

2) **User Filing e-FIR:** The user interacts with SI by entering ID for validation, which is done on run-time basis from the citizen's national database as it is connected with the SI, and allow him/her for filing an e-FIR in case of cognizable offenses only. If the user had filed e-FIR and it is still pending, then he/she will not be allowed to modify it, as it will result in change in the original hash value, which indicates changes made to the original e-FIR data that would help in identifying fraud. The user will have to provide all the following details when filing an e-FIR (with any additional information if any).

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

3) **Admin Approving e-FIR Transaction:** The admin will be responsible for authorizing all the transactions on blockchain. When user files an e-FIR, the admin of police station assigns one of the investigating officers to verify the information provided by the user, check the originality of evidences and solve the case. If the data is found to be valid, the admin generates a hash of that e-FIR data and uploads

Fig. 3: Transaction of a single block in Ethereum blockchain (Ganache).

it on the distributed private blockchain using smart contract. Also, the e-FIR details provided by the user are uploaded to the police station central database digitally signed with the exact hash generated for that e-FIR data. The hash will account as an ID for the e-FIR. If e-FIR data is found as fraud, the admin will not approve the transaction and hence, the case and the transaction will be dropped.

4) **Handling False e-FIR:** If the user or admin of police station intentionally tries to register false e-FIR against someone, then the accused user will have the privilege to request to the SP for an auditing of false e-FIR. The SP has access to the hash data and all other details of the case such as the city and police station, admin of the police station, investigating officer, and e-FIR data, which is allegedly filed against the accused user. As the credentials of all involved persons who have filed alleged e-FIR, are saved on blockchain in the form of hash, they are unable to withdraw their identities from blockchain ledger to vanish the evidence of not being involved in the case. Blockchain also stores the time-stamp of every block transaction, which can further aid in identifying the involvement of a person in fraudulence.

IV. Implementation and Results

We have created a local database of e-FIR data in Matlab and that local database is interfaced with Ethereum blockchain using the intelligence of smart contract. The details of our proposed model implementation is explained below.

A. Platform Interfacing

In a P2P interfacing, we have connected Matlab with Python IDE, and eventually, the Python IDE is connected with Ganache [17], which is a tool used for Ethereum blockchain. We have deployed the smart contract on Ethereum online Remix IDE [18]. The smart contract is deployed on a Web3 Remote Procedure Call (RPC) environment using a specific port number. Python IDE receives data from Matlab (database) on that specific port number, which then forwards the data to Ganache (Ethereum Blockchain). The port number of Ganache IDE should be set to the same port number used by Matlab, Python and Remix IDE [20]. Complete details of e-FIR data stored in single transaction on blockchain is shown in Fig. 3.

B. Ethereum Blockchain

We have used Ganache software for Ethereum blockchain, which is a development tool provided by Ethereum developers. The benefit of using Ganache is that it provides 10 different accounts with each account having 100 ethers, and the purpose of those ethers are merely for development purpose. For the scalability of the system, we need to build and implement personal blockchain, where we can generate multiple unique addresses for every single node. The benefit of personal blockchain is that, if we define an authority for mining the block, then the mining process becomes very fast, because the authority is only responsible for utilizing computational power for mining the block. The mining process of Ethereum uses PoW concept; however, defining functions in a smart contract and allowing specific addresses to specific operations can provide the benefits of PoA. Specifically, in our model, we have made some addresses as an authority that can do specific operations, which other addresses can not do, i.e. registering all the police stations from SP node address, and approving e-FIR transaction from admin node address.

The more number of registered e-FIRs in police station database, the more number of transactions occur on blockchain ledger using smart contract, as shown in Fig. 4. The graph is plotted against SHA-256 hashing algorithm (more details can be found in Section IV.C).

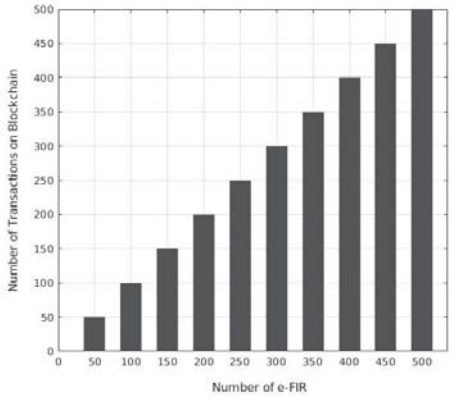

Fig. 4: Number of transactions vs. e-FIRs on blockchain.

C. Smart Contract

In our model, we have developed smart contract in a solidity programming language in Remix IDE used for Ethereum

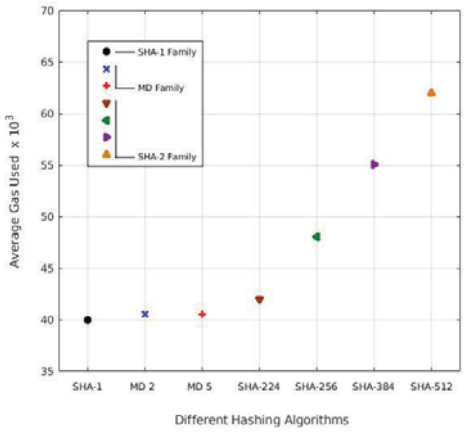

Fig. 5: Different hashing algorithms.

blockchain, which gets data in the form of hash and stores it on the blockchain. The functions in smart contract contains the following functionalities as discussed in Section III.

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

We have used a number of different hashing algorithms in the implementation of the proposed blockchain-based framework to test the impact of these hashing functions on the performance of our proposed framework. We used the Secure Hash Algorithm (SHA) family and the Message Digest (MD) family of hashing algorithms. Specifically, we used SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, MD-2, and MD-5. Gas in Ethereum is defined as a special unit that measures the amount of computational effort that it will take to execute certain operations. From the results obtained, as shown in Fig. 5, the minimum average Gas used by SHA-hashing family is 40,000 and maximum Gas being used is around 62,000. Likewise, the average Gas used by MD-hashing family is 40,500. SHA-512 (512 bits) is considered to be the most advanced and secured hashing algorithm, but it uses more Gas, as shown in Fig. 5, resulting in less transactions per block in blockchain. On the other hand, using SHA-1 (160 bits) can benefit us with more transactions in a single block, but with less hashing security, as SHA-1 is not as much secure as SHA-512 is. Using SHA-256 (256 bits) could endeavor data integrity by having sufficient hashing security level while using moderate Gas value, as observed in Fig. 5.

D. System Specifications

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

Table II: SYSTEM SPECIFICATIONS

System RAM	8 GB DDR3
Hard Drive	128 SSD/640 HDD
System Core	Intel Core i5
Operating System	Ubuntu 18.04

V. Conclusion And Future Work

This paper examines the relatively under-developed area of record management in police stations for the prevention of data tampering and false report filing, using the concept of blockchain technology. Research conducted in this paper has presented a consensus based solution for providing integrity to the offenses data stored in police station database using blockchain. In the proposed framework, Matlab is interfaced with Ethereum blockchain using Python and Web3 RPC to intelligently secure the e-FIR data transaction through smart contract. Multiple simulations have been performed to demonstrate the trade between number of transactions occur in a single block and different hashing security level for e-FIR data.

The proposed system will further be investigated in future for dynamically selecting different hashing algorithms based on classification and criticality of the offenses data. The system will also efficiently utilize the Gas value in Ethereum blockchain by identifying the offense's data type and its importance, in order to maximize the number of transactions stored in a single block.

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.