Blockchain driven Evidence Management System

Shyam Mehta
Data Science and Business Systems
SRM Institute of Science & Technology
Chennai, India
sm6159@srmist.edu.in

K. Shantha Kumari
Data Science and Business Systems
SRM Institute of Science & Technology
Chennai, India
shanthk@srmist.edu.in

Paras Jain
Data Science and Business Systems
SRM Institute of Science & Technology
Chennai, India
pj6337@srmist.edu.in

Harshal Raikwar
Computer Science and Engineering
SRM Institute of Science & Technology
Chennai, India
hr5359@srmist.edu.in

Shubham Gore
Data Science and Business Systems
SRM Institute of Science & Technology
Chennai, India
sp8226@srmist.edu.in

2023 3rd International conference on Artificial Intelligence and Signal Processing (AISP) | 979-8-3503-2074-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/AISP57993.2023.10134799

Abstract—**When a cognizable violation 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. Indian government launched nation-wide Crime and Criminal Tracking Network and Systems (CCTNS) during 2009 and it is an efficient e-governance system. This paper provides a blockchain solution to handle the complaints given on both cognizable and non-cognizable complaints. Using real-world examples from previous events, the technology and security underlying the use of blockchain will be discussed. Police will file an e-FIR, which will be validated by the authorities, and on acceptance of the FIR, it will be encrypted and stored as a hash along with the timestamp and hash of the next block. Now, how blockchain makes it secure is that it doesn't let anybody make changes to the FIR without proof of work and a vote of consensus in which a majority of the blockchain must agree to the change. The hash will be stored in smart contracts using Ethereum. Our findings demonstrate a trade-off between the number of transactions contained in a single block on the blockchain ledger and the security level of various hashing algorithms for the offence data.**

Keywords – *e-FIR, Blockchain, Encryption, IPFS, Ethereum, Cryptography, Data Integrity*

I. Introduction

A crucial idea behind smart cities is information and communication technology (ICT). By fostering economic growth, sustainable good governance, prudent resource management, effective mobility, and protecting citizens' privacy, ICT invests in human social life to improve citizens' quality of life. The use of numerous sources and an estimate of the number are required because no single organization collects verifiable information about exonerations due to erroneous convictions, and even if they did, we could not know about the cases that were not exonerated. Our findings demonstrate a trade-off between the quantity of transactions included in one block of blockchain ledger and the security level of various hashing algorithms for the offences data.

Each Police Agency that implements blockchain builds a network of dependable Nodes and receives the most recent version of the blockchain ledger as they go. Every time a piece of evidence is hashed and recorded, a new block is created and immediately moved to the blockchain and copied in all Nodes. This ensures that it is not possible for any agency to ever change the blockchain of evidence without being immediately discovered by the others because their copies will not match and break the chain. All users are identified and have credentials because this is a private, federated blockchain. To address issues with denying police officers the ability to register complaints, we suggest an online system for managing police complaints that uses blockchain technology to manage FIRs and NCRs in a decentralized manner. Blockchain technology is a distributed and decentralized data structure that holds all the legal transactions in connections of blocks and is based on a peer-to-peer network topology. Satoshi Nakamoto's invention, bitcoin [5], is the first use of blockchain technology. The primary goal of blockchain is to ensure that only genuine blocks are added to the chain, meaning the block must have a certain number of votes or consensus. Smart contracts are written into computer codes and represent agreements between two parties. There is no need for a third party to handle it. Similar to a standard contract, smart contracts function by allowing certain codes to be added directly and for the parties concerned to review them prior to the deadline. Certain terms and conditions of these contracts must be upheld.

The two main contributions in this study are as follows: First, a blockchain-enabled architecture is developed that effectively ensures the integrity of e-FIR data and may be used in a smart city setting. Second, by leveraging the blockchain concept and smart contracts to resolve it, false Registration of the e-FIR is reduced to a minimum. This is an effort to use blockchain to prevent fake registration and give e-FIR data integrity. We frequently offer a decentralized program that monitors all actions related to police complaints that are pertinent to this situation. from the time a complaint is made until the court receives an accusation and trial begins.

Blockchain technology is used to bring the confidence to the people who are giving complaints and the police department. The system is protected against data loss as well as brute force hacking and other harmful assaults. The following sections are organized as following:The remainder of the essay is structured as follows: Section II talks with e-FIR and pertinent methods there. Presented in Section III is the suggested system design. Results of the proposed Framework's implementation and assessment are displayed in Section IV: In Section V, the final thoughts and suggestions for future work are provided.

Information and communication technologies (ICT) are a key component of the concept of smart cities. ICT invests in human social life to improve the life's quality metrics of the people by ensuring growing economy, Steady & good governance, intelligent resource management, and efficient mobility, while also ensuring citizens' security and privacy. Because no single organization gathers verified information about exonerations owing to mistaken convictions, and even if they did, we are unable to know about the cases that were never exonerated, the applications of maximum sources and an approximation of the number are necessary.

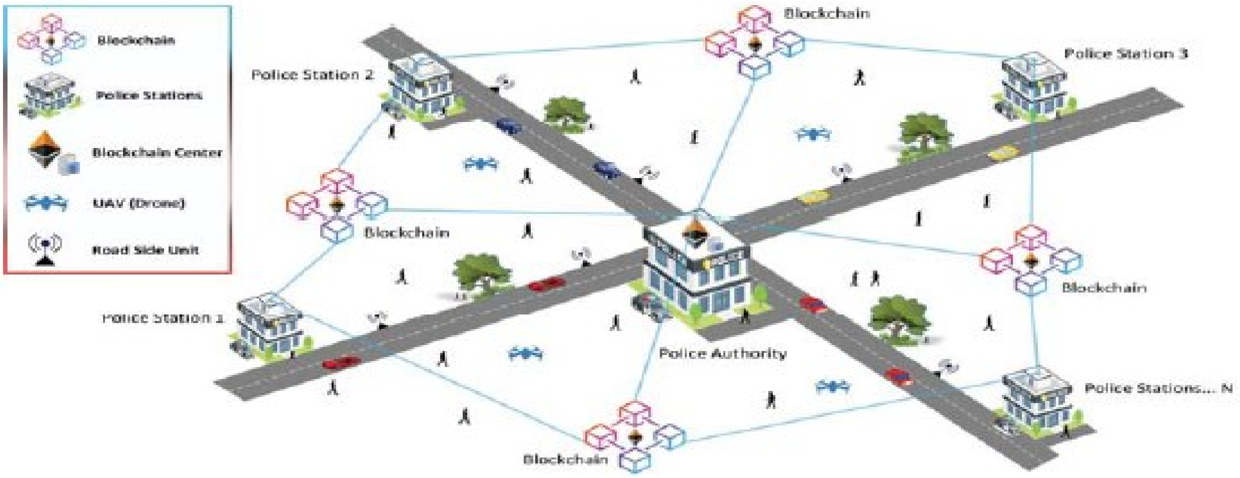

Fig. 1: System model of smart police stations in a smart city environment.

II. LITERATURE SURVEY

The authors in [9] proposes Blockchain secured FIR system. This paper proposes a system that provides a secure FIR system that tries to make system simple and efficient. As this eliminates the intermediate person and forms a system that contains only Police and Public which can eliminate the fear of trust. The system has four stakeholders i.e., the person lodging complaints, the person who is the witness, the investigating officer, and the accused. A decentralized network is built that does not rely on trust. As a result, the registered user can submit a complaint from any internet-connected device. We can say that the network will be free of corruption because the blockchain will make it more secure, immutable, and decentralized.

The researchers - K. Tabassum, H. Shaiba, S. Shamrani and S. Otaibi [10] provide not only a simple but user-friendly interface that will make it easier and faster for citizens to communicate with security services. It is possible to report a crime or submit a complaint online from any location. Additionally, officials at the police department have access to the report, which enables them to take any necessary actions to address the complaint or crime.

An electronic police system is proposed in [11] aims to speed up and simplify the registration and tracking of FIRs. As a result, this may benefit both the public and the police. Additionally, the complainant receives direct notification of updates regarding case details through the application.

The authors in [12] proposes a completely integrated and compact system that can be used by the public as well as police. As this system can benefit both. Also, SOS is extremely useful and an efficient security measure. This system offers new features as well as retaining the original characteristics of the existing systems.

The authors in [13] aims at eradicating the barriers of the manual police system. For which they proposed a system that can provide the user an option to file a complaint or FIR anonymously. In addition, a password system has been added to documents so that only police can access the relevant file.

In paper [14], the authors propose a system that is highly secured and easily accessible as police have their database from where they can gather all the information and have biometrics like facial or fingerprint recognition. Apart from this they also have Wireless Sensor Network in traffic systems, like e-driving license. Certainly, this way we can have a proper structured system to improve and speed-up the police's working system.

The work titled “Smart Complaint Management System,” [15] talks about a system where if any customer find any company not providing proper service then they can file a complaint against them via chatbot which later classify them and also generates data visualization for the summary of the complaint.

The work in [16] elaborated a real-time crime records management system for national security agencies. This proposal includes a computerized crime record management system that helps the National Police Force (NPF) manage criminal records more effectively and effectively, allowing it to make better decisions and increase its reliability, which in turn helps lower crime rates and boost national security.

The authors in [17] proposes how blockchain helped to create a numerous application in various fields. The main and most useful characteristic of this blockchain system is that it is decentralized and takes information of each user and with its agile and minimum time of response it provides all the important information to the participants instantly.

The research work explained in [18] details about “Online Criminal Record Management System,” and this system provides us with the recording of every crime recorded with proper date and time details. This system's main feature is that it offers a straightforward, user-friendly, cost-effective, and effective online crime recording system with a clear and understandable web interface. In general, it addresses all issues pertaining to crime reports, specifics about criminals, and their crimes.

A straightforward and simple FIR filling system is provided by the work presented in [19], which organizes all criminal records in a centralized database. Apart from this it will also provide them all the updates they seek regarding their FIR.

The authors in [20] proposes a system that provides solution to biggest drawback of current judiciary system which is the communication gap which with this system would not be a problem anymore as this application automatically adds all the updates of users FIR and not only that it also overcome the problem of fake FIR as user has to provide all the required verification documents. But the only drawback of this system is that it requires GPS and Internet connection 24x7.

III. PROPOSED FRAMEWORK

The suggested solution uses several technologies, such as IPFS and blockchain, to manage complaints on a decentralised platform. The system's implementation is explained after the system's elaborate design is laid out in the form of modules. The proposed intelligent framework makes use of the advantages of blockchain technology to address a significant problem—namely, how data 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 blockchain's important properties include making the system decentralized and allowing anyone to change the system only with a vote of consensus and valid proof of work.

A. Proposed blockchain model

The unique framework that is expressly proposed in this paper has two components:

- A tamper-proof and fraud-resistant intelligent system that uses distributed blockchain ledgers and smart contracts is presented to care for the integrity of e-FIR. (IPFS is an alternative of Ethereum)
- The user as well as the admin's credentials are gathered and stored in the blockchain for auditing purposes in order to combat false e-FIR registration.

Public Ethereum is the blockchain that was used in a network that utilizes the proof-of-work principle. Ethereum gives transparency in addition to encryption, ensuring privacy of sensitive information. Program for smart contracts generates immutable data while running on the Ethereum network, which ensures that only compliant transactions are recorded in the ledger. The contact has committed to the network. The encryption method used in the complaint is described in detail. The security module and the user-provided proofs are saved within an open IPFS network. Ethereum's transparent nature ensures the complaint is present on the blockchain.is accessible to any network participant. In addition, preserve discretion and follow the security procedure. module is put into action. On the blockchain network, the hash corresponding to the proofs and the encrypted complaint information are saved. A police officer who is already a part of the network can invite more officers to join. This makes sure that the reports and crime statistics are only accessible to authorized police officers. The police then render the FIR as a pdf and encrypts it using a similar process described in the security module. The appropriate hash is subsequently recorded on the Ethereum network, and this encrypted document is then stored on the IPFS network. The proposed model of evidence management system can be seen in Fig. 2

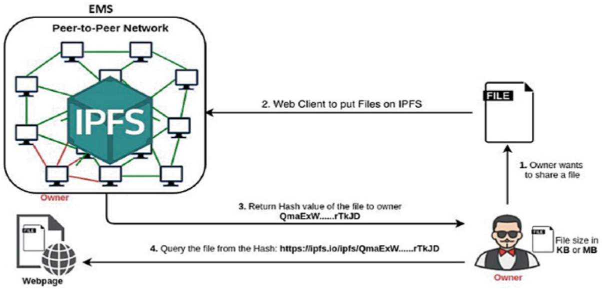
EMS
Peer-to-Peer Network
IPFS
Owner
2. Web Client to put Files on IPFS
FILE
1. Owner wants to share a file
3. Return Hash value of the file to owner QmaExW......rTkJD
4. Query the file from the Hash: https://ipfs.io/ipfs/QmaExW......rTkJD
File size in KB or MB
Owner
Webpage

Fig 2. Evidence Management System using IPFS

B. Architecture Diagram

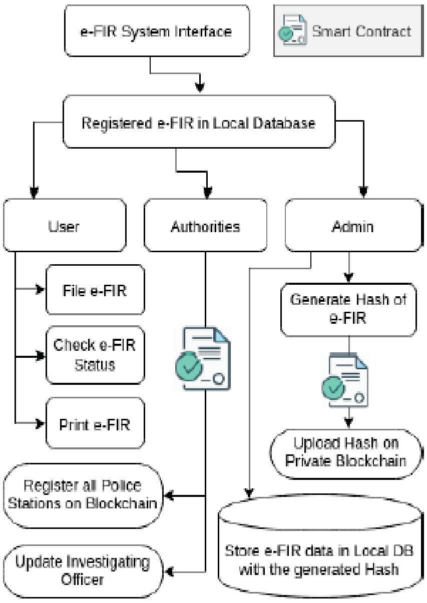
e-FIR System Interface
Smart Contract
Registered e-FIR in Local Database
User
Authorities
Admin
File e-FIR
Check e-FIR Status
Print e-FIR
Generate Hash of e-FIR
Upload Hash on Private Blockchain
Register all Police Stations on Blockchain
Update Investigating Officer
Store e-FIR data in Local DB with the generated Hash

Fig.3 Workflow diagram

Encryption

For its public-key cryptography, Ethereum uses the ECDSA (Elliptic Curve Digital Signature Algorithm). Bitcoin and this are equivalent. Public-private key pairs are used in public-key cryptography (asymmetric cryptography). The method of changing your private key to a public key is simple, but the process of converting a public key to a private key is challenging. In essence, every public key has a private key connected with it (there is no algorithmic way to do this currently, so you just must guess; it requires an immense number of computations). You can share your public key with anyone without worrying that they will be able to figure out your private key from it as a result. The prime number theorem, which depends on the fact that we have not found a way to effectively describe the distribution of prime numbers mathematically, is used by RSA, another type of public key encryption that you may be familiar with, to reduce computing complexity.

The Discrete Logarithm Problem, an alternative approach to computing computational complexity used by ECDSA, is based on the impossibility of estimating the discrete logarithm of a random point on the specified elliptic curve.

Using ECDSA instead of RSA is advantageous since it offers comparable security to RSA while requiring fewer key sizes. The computational difficulty of the 256-bit public key in ECDSA is equivalent to the computational complexity of the 3072-bit public key in RSA.

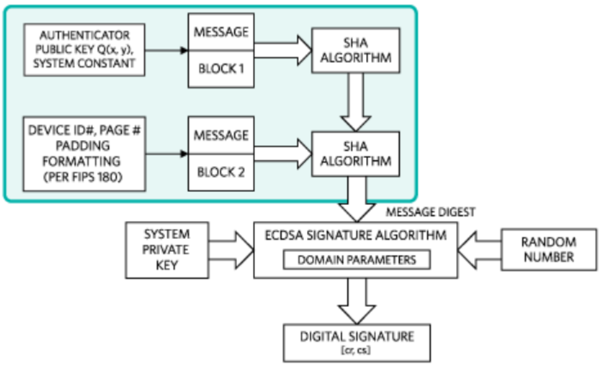

Fig.4 ECDA Signature Algorithm

C. Blockchain Module

The FIR, NCR, and Chargesheet, which are legal documents that are covered in Section 1, are available to the complainant, the police, and the suspect. Since the transactions are broadcast to every node, there is bottleneck while using the public blockchain.

The information that must be saved on the blockchain network is encrypted for this purpose by our system. A 16-bit ECDA or AES both can be used for the encryption. To exchange secret keys, one uses the Diffie Hellman key exchange algorithm.

The implementation details of this module (Fig. 1) is explained as follows:

(a) A security pin must be added every time a new complainant or police officer registers in the system (a/b). The database contains the security pin's hash.

(b) The public components used in the Diffie Hellman key exchange technique are the security components (prime number p, base g, A, and B) that are stored in the database. Following is the formula used to determine A and B:

$$A = g^a \bmod(p), \quad B = g^b \bmod(p)$$

(c) A secret key is used to encrypt a complaint that is registered by a complainant. The security pin (a) and the public components of the police station (p, g, and B) are used to calculate the secret key.
(d) The complaint is added to the blockchain.

Now, the block chain we are using the public Ethereum network it is based on the concept of proof of work. If anybody from the investigating officer or anybody wants to make a change in the documents, one has to go through the whole process. The Ethereum blockchain's smart contract software generates an immutable record and ensures that only transactions that adhere to the contract are published to the network. The security module's described mechanism encrypts the complaint's specifics, and the user-provided proofs are kept on a public IPFS network. Due to Ethereum's transparency, all users of the network may see the existence of the complaint on the blockchain.
The police officer who is a participant of the network can add another officer to the network. This ensures that only an authenticated police officer has access to the reports and crime data. Authenticated officers can make a change in the network by providing proof of work and vote of consensus (which is more than fifty percent people should be able to agree to the change one is proposing).

IV. Implementation And Results

Using the intelligence of the Moralis SDK, which provides us with the IPFS data storage space, we have created a local database of e-FIR data in Firebase. The implementation of our proposed model is described in detail below.:

a. Platform Interfacing:

We have connected Firebase with Javascript in a P2P interface, and eventually, Node.js is connected with the Moralis SDK, which gives us a database. A specific port number is used to install the smart contract in a Web3 Remote Procedure Call (RPC) environment. On that particular port number, Javascript receives data from Firebase (the database), which then forwards the data to IPFS (the Ethereum Blockchain). It is recommended that IPFS use the same port number as Firebase and Node.js. A single transaction on the blockchain stores all of the details of the e-FIR data.

b. IPFS:

We used the Moralis SDK, which offers developers from all over the world top-notch APIs for data storage, integrating blockchain into their solution stack, and scaling with ease. Utilizing IPFS has the advantage of using content-addressed storage and decentralized protocols. Each item of data in this protocol is given a special content identifier (CID). Based on this specific CID, all content-addressed data in IPFS can be located and retrieved. Each resource in IPFS is given a distinct CID, and these CID files are immutable, meaning they cannot be changed by any outside entity. IPFS additionally makes use of transit encryption to secure data as it is sent between IPFS nodes. Compared to HTTP, this gives much greater security benefits. The immutable resource structure of IPFS dramatically reduces several cybersecurity concerns.

In order to store and share data with IPFS, multiple peers are simultaneously queried for the data. This decreases bandwidth consumption. The quickest and most efficient way to provide content to a user is for IPFS to simultaneously retrieve data from many nodes based on the CID of the user's request. The location of content storage has been changed, and it is no longer connected to distant servers. Studies show that this method of information retrieval can reduce the amount of video bandwidth used by up to 60%. With IPFS, large volumes of data may be distributed quickly and duplicate-free. The CID generated by IPFS offers a digital fingerprint that can ensure validity and uniqueness. This facilitates deduplication by generating a single instance of data with an immutable CID.

Additionally, because there is only one copy of each resource, authentication is considerably simpler. Since there is no duplication, IPFS reduces the amount of storage space required for data backups and archives. Any organization that archives its data would benefit greatly from this. IPFS greatly increases the power of content creators. Without relying on a third-party content distributor, creators can disseminate their own work. Additionally, creators are not required to invest on servers to manage their content. Anyone can upload content to the IPFS network, and anyone in the world can safely access that content. So, using IPFS, we were able to store all our data securely and read it using Firebase.

c. Firebase:

This is the main memory or say storage area where all our details will be replicated. As we have connected our localhost as well as the IPFS with Firebase it will store user's login credentials as well as the user's FIR details. Firebase is the toolset that helps any app to build, improve and grow. Analytics, authentication, databases, configuration, file storage, push messaging, and other features are also included. Consequently, because of these characteristics, it is ideal for this system.

d. Node.js:

As IPFS and Firebase helped us to get a better backend and storage, respectively. Javascript helped us to connect them with the frontend as it is equally important as the backend. As to create user-friendly it is equally important to have a clean and well-structured frontend to not only make users know the website better but also to attract more and more users.

e. System Specifications:

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

Table I: 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

The paper discusses the problems of data tampering and the lack of the security in the current record management system used by the police department. Paper tries to propose a solution for the problems using block-chain and offers an alternative, which is much more efficient and secure. The research described in this paper has suggested a consensus-based method for leveraging blockchain to ensure the integrity of the offences data kept in police station databases. The suggested system will offer while still maintaining the privacy of the stored data. Additionally, knowing that the police cannot disregard their complaints may encourage people to come forward and make them. By making the laborious process of submitting reports like FIRs simpler, it will also be advantageous to police officers. In our system, the frontend is based on React.js and backend is on Node.js. Also, in this paper Ethereum has been used as a block chain network with firebase as the database.

The stakeholders' degree of trust is not necessary for the decentralised network to function. We put up a strategy that will defend against dishonest police behavior and provide justice right away. Future research into the suggested system's ability to dynamically choose different hashing methods based on the categorization and criticality of the offence data will be conducted.

REFERENCES

1) Derick Anderes, Edward Baumel, Christian Grier, Ryan Veun, and Shante Wright "The Use of Blockchain within Evidence Management Systems"

2) Revathy Sathyaprakasan Pratheeksha Govindan ,Samina Alvi ,Lipsa Sadath ,Sharon Philip ,Nrashant Singh "An Implementation of Blockchain Technology in Forensic Evidence Management"

3) Kim, D., Ihm, S. Y., & Son, Y. (2021). Two-level blockchain system for digital crime evidence management. *Sensors*, *21*(9), 3051

4) Rao, S., Fernandes, S., Raorane, S., & Syed, S. (2020, June). A Novel Approach for Digital Evidence Management Using Blockchain. In *Proceedings of the International Conference on Recent Advances in Computational Techniques (IC-RACT).*

5) Leible, S., Schlager, S., Schubotz, M., & Gipp, B. (2019). A review on blockchain technology and blockchain projects fostering open science. *Frontiers in Blockchain*, 16.

6) Design and Implementation of an E-Policing System to Report Crimes in Nigeria

7) Aditya Jain, Divij Bhatia, Manish K Thakur's "Extractive Text Summarization using Word Vector Embedding"(2017).

8) [8] Hingorani, I., Khara, R., Pomendkar, D., & Raul, N. (2020, December). Police complaint management system using blockchain technology. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 1214-1219). IEEE.

9) Gupta, Antra and D. V´ılchez Jose. “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

10) K. Tabassum, H. Shaiba, S. Shamrani and S. Otaibi, ”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

11) Iyer A, Kathale P, Gathoo S and Surpam N 2016 E-Police SystemFIR Registration and Tracking through Android Application International Research Journal of Engineering and Technology 3(2) 1176-1179

12) P. A. K. S. Y. K. S., Shivaganesh Pillai, “Online Fir Registration and Sos System", int. jour. eng. com. sci, vol. 5, no. 4, Dec. 2017. Omoregbe, Nicholas Misra, Sanjay Maskeliunas, Rytis Damasevicius, Robertas Adesola, Falade Adewumi, Adewole. (2019)

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

14) 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

15) 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

16) Onuiri, Ernest Oludele, Awodele A, Olaore O, Sowunmi A., UgoEzeaba. (2015). A Real-Time Crime Records Management System for National Security Agencies

17) A. T. Dini, E. Gabriel Abete, M. Colombo, J. Guevara, B. S. Mench´on Hoffmann and M. Claudia Abeledo,” Analysis of implementing blockchain technology to the argentinian criminal records information system,” 2018 Congreso Argentino de Ciencias de la Inform´atica y Desarrollos de Investigaci´on (CACIDI), Buenos Aires, 2018, pp. 1-3, doi: 10.1109/CACIDI.2018.8584365 .

18) Pratibha Mishra,Ghousiya Bee. N2, Mohsina S3, Mubashshira Sultana, Surbhi Singh, “Online Criminal Record Management System,” International Journal of Engineering Science and Computing, vol. 9,no. 5, May 2019.

19) Archana M, Durga S, Saveetha K, “Online Crime Reporting System,” Int. Jnl. Of Advanced Networking Applications (IJANA), https://www.ijana.in/papers/82.pdf.

20) S.P. Godlin Jesil,Rajat Basant, Pratishvir, “crime reporting system using android application,” International Journal of Pure and Applied Mathematics, vol. 119,no. 7, 2018, Https://Acadpubl.Eu/Jsi/2018-119- 7/Articles/7a/56.Pdf