Smart FIR lodging architecture with the help of blockchain and IPFS

[1]Soham Banerjee 201010250, [2]Anubhav Garg 20100007, [3]Sudhanshu Tripathi 201010252
[1 & 3]Department of Electronics and Communication Engineering, [2]Department of Computer Science and Engineering, Dr. S P Mukherjee International Institute of Information Technology, Naya Raipur-493661, Chhattisgarh, India
Emails:[1]soham20101@iiitnr.edu.in, [2]anubhav20100@iiitnr.edu.in, [3]sudhanshu20101@iiitnr.edu.in

Abstract — **The most crucial smart service, among many others, which India must have to adopt is a smart and robust policing system. In Indian law, any offense, whether cognizable or non-cognizable, an FIR has to be lodged with the Police Station for any further action. In some cases, where a complaint case is filed, FIR can be ignored. The significant gap in the police-population ratio exists.Often it is not possible to visit the nearest police station from the place of occurrence of the offence.Lack of coordination between various states and law enforcement agencies.Investigations may get influenced behind the scene.**
Evidence, forensic reports and investigation case files may be tampered with.Every procedure is handwritten or electronically written, and there might be a chance to mutate the data. It is sometimes seen that they ask for a bribe to take further action. It is also seen that they modify and delete the data in someone's interest. This results in a wrong judgment by the judiciary, and one didn't get justice. The one who committed the crime is released. This results in a loss of faith in the police system and police officials, and even in the judiciary. Delay in investigation and lack of transparency. Our constitution, Indian Penal Code, and Criminal Procedure Code have given enough power to police officers to take necessary actions to maintain law and order. However, there is a flaw. Some corrupt officials somehow misuse this power and threaten ordinary people. In some cases, police officials refuse even to lodge the FIR. It is often seen in cases where rich and powerful people are involved.

***Keywords*— Blockchain, IPFS, Smart contract, Smart policing, Digital FIR.**

I. INTRODUCTION

The most crucial smart service, among many others, which India must have to adopt is a smart and robust policing system. In Indian law, any offense, whether cognizable or non-cognizable, an FIR has to be lodged with the Police Station for any further action. In some cases, where a complaint is filed, FIR can be ignored. The significant gap in the police-population ratio exists.Often it is not possible to visit the nearest police station from the place of occurrence of the offence.Lack of coordination between various states and law enforcement agencies.Investigations may get influenced behind the scene.

Evidence, forensic reports and investigation case files may be tampered with.Every procedure is handwritten or electronically written, and there might be a chance to mutate the data. It is sometimes seen that they ask for a bribe to take further action. It is also seen that they modify and delete the data in someone's interest. This results in a wrong judgment by the judiciary, and one didn't get justice. The one who committed the crime is released. This results in a loss of faith in the police system and police officials, and even in the judiciary. Delay in investigation and lack of transparency. Our constitution, Indian Penal Code, and Criminal Procedure Code have given enough power to police officers to take necessary actions to maintain law and order. However, there is a flaw. Some corrupt officials somehow misuse this power and threaten ordinary people. In some cases, police officials refuse even to lodge the FIR. It is often seen in cases where rich and powerful people are involved.

To solve this particular problem in the complaint system, blockchain technology is introduced. Using blockchain technology, any data that is written in the block cannot be changed at any time. Moreover with the help of consensus in a random group, one can guarantee the decentralized nature of the proposed blockchain-based application in this particular field.

It aims to increase the accountability, transparency, and trust concerning the storage, safeguarding and sharing of evidence and intelligence related to ongoing investigations, criminal cases and justice information among the stakeholders. It allows the citizens to interact with law enforcement agencies securely (even without visiting them physically) and to avail all related services.

An popular example of police misconducting to refer for your case :- Police mishandling evidence is the O.J. Simpson case. In the O.J. Simpson investigation for the murder of Nicole Brown, the police botched the collection and processing of crucial evidence. His criminal defense team was able to win his case based largely on mishandled evidence.Just one example of mishandled evidence was the handling of O.J. Simpson's blood. His blood was drawn very early in the investigation by police. The police did not document how much blood they drew, and the person who drew the blood said they thought they drew 8mL. Only 6mL of his blood was accounted for. This let the defense team argue that the blood was at the very least mishandled and, therefore, unreliable evidence. At worst, some may have been planted.

II. OBJECTIVE OF ARCHITECTURE

The architecture is aimed at providing ease at lodging FIRs or file the case without unwanted hindrance from mid-level service. It not only ensures proper security on the side of the user, it also streamlines the methodology of FIR processing on the law enforcer's side. All in all it will be a boon for everybody. Authors performed thorough research on improving the policing conditions of our country. But ultimately the solution came down to handling the issue in a modular approach. Hence the focus is just solving the FIR lodging problem.

III. RELATED WORKS

Hingorani et al.'s research paper titled "Police Complaint Management System using Blockchain Technology" talks about using technologies like Blockchain, IPFS, and Hashing techniques to store and keep track of detailed records of police complaints filed by complainants and data handling history in form of an immutable ledger. Inter-Planetary File System is a peer-to-peer network for storing and sharing data in a distributed file system. The proposed idea was to store more and more information about data surrounding the FIR, such as launch date and timing, proof of FIR filing, and agreements made, apart from storing each and every detail about the FIR itself. Thus this ensures a partially trustless environment for both the law-enforcer and the complainant under the idea that both parties are safeguarded by immutable proof-recordings of the function once exercised. Thus one cannot think of denying the act performed in any way anytime in the future. If so happens, lawful actions can be taken against law enforcement agencies (namely the policemen) as a fundamental right.

The drawbacks are that the proposed idea is impractical and overly simplified for practical use. It focuses on penalizing the law-enforcer and is unethical to put the policemen under the spotlight only, rather than looking to completely unroot the scope of mishandling FIRs. This can lead to an infinite cycle of complaints in case of dissatisfaction of the complainant and lead to misuse of the right as well. The area this proposed system focuses on is too narrow, i.e. the case when FIRs are later denied importance and termed as vague and unrelated in the future when the matter cools down. But other important problems that the current FIR lodging system brings with itself like denying lodging a complaint itself under the bias of a particular individual involved in the complaint. This is a much bigger problem as this leaves no trace of the happenings in any government record and is dangerous for society in all aspects. This happens because of the powers the law enforcement agencies have been bestowed upon, which they misuse in some cases. The sole purpose of introducing blockchain should be to sedate this concentrated power which would solve many of the problems.

Arnab Mukherjee et al.'s paper titled, "PoliceChain: Blockchain-Based Smart Policing System for Smart Cities" talks about Hyperledger technology besides the use of IPFS for storing data. Now the kind of data authors talk of storing in the IPFS is not only FIRs but investigative findings, forensic and case reports, updates, and basically every intricate detail related to the investigation of police cases and not just FIR filings. This

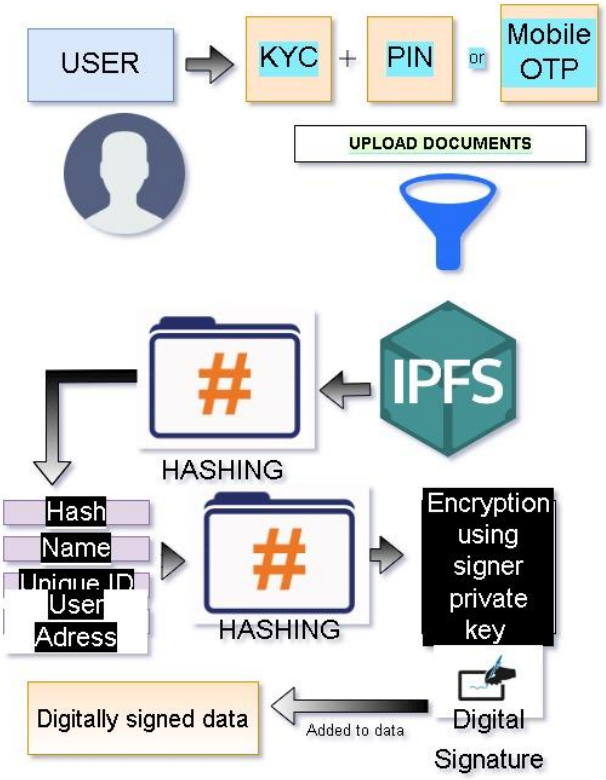
would help the police and law enforcement agencies immensely and the focus is more on that i.e. to maintain a lossless record of active investigations. Taking the police investigation records from the pen and paper-based police file stage to immutable, secure digitized mode is the main objective of this paper. Although the objective is not completely aligned with the use case we are targeting, it still can be sought as a reference to learn about the usage of IPFS's applications for investigative purposes. Though a drawback that has been highlighted by the authors themselves is that the paper is in the proposal stage. Moving on to the next reviewed related works.

Hassija et. al's paper titled, "Police FIR Registration and Tracking Using Consortium Blockchain ", talks about consortium blockchain and partly-decentralized functioning of lawful FIR lodging. This paper proposed the creation of a mobile application to digitalize the process of FIR lodging besides other activities in a safe and secure manner. The proposed architecture is, Clients i.e. common citizens will provide FIR information; policemen will provide case details and updates on opened investigations. These bits of information will constitute a block. Now clients and law enforcement agencies will be a part of the same blockchain and hence, the proper distinction of information sharing levels among the various categories of application users should be made with proper clarification. To ensure this, consortium blockchain is introduced by the authors in the architecture. Blocks will be mined only by eligible block miners and not all network participants. Blocks after generation go to the Commissioner for verification round, and then on passing verification, it is commanded by the commissioner for the mining round.

Drawbacks are the scarcity of client node verification stages to ensure that the scope of fake FIR registration from invalid nodes is banned from the network. Now what is invalid and what isn't, is a thing that needs a proper definition, none of which is taken up in the discussion of the proposed architecture.Commissioner nodes act as a fairly centralized entity in the network and this right can again be misused as trust is yet not entirely removed from the architecture which defeats the purpose of the application of blockchain in the system. Lastly, one big issue with the architecture is that the system proposed takes into account idealistic measures which only means if one were to implement this in the existing system, it would need a complete overhaul of the current architecture. An alternative measure that can fit right in like the loose end of a puzzle in the existing system is more desirable and our aim is to do just that. Now let's see how it is performed in the later discussions. A tabular comparison is laid out as below.

III. PROPOSED METHODOLOGY

The legal documents i.e. FIR/NCR/Chargesheet are available to the suspect, police, and the complainant. The use of public blockchain becomes a bottleneck since the transactions are broadcasted to each and every node. For this, our system encrypts the details that are to be stored on the blockchain network. The encryption is done with the help of a 16 bit AES algorithm (Symmetric-key cryptography). The Diffie Hellman key exchange algorithm is used to exchange secret keys. But the entire data is not encrypted. Instead specific fields like Suspect name, Age, Height, physical or identifiable features to save suspect's identity till mining (hypothetically). The AES key will be stored securely till then. Only after mining, will the key be sent to the concerned Police station head commissioner and officials. Thus while filing a complaint, it will become next to impossible for the police to differentiate a complaint filed against Mr. X vs that filed against Mr. Y. For the police it will always be like for example, this crime has allegedly happened and it is on some Mr. Anonymous. The identity will be revealed only afterwards as described earlier, to ensure the further investigation procedure to happen.



The following explains the implementation details of this module . Whenever a new complainant/police officer registers in the system, he/she has to add a security pin (a/b). The hash of the security pin is saved in the database. The security components (prime number p, base g, A and B) stored in the database are the public components involved in the Diffie hellman key exchange algorithm. A and B are calculated by the following formula: When a complainant registers a complaint, The complaint is encrypted with the help of a secret key. The secret key is calculated with the help of public components of the police station and security pin . The complaint is added to the blockchain. The system decrypts the complaint (on the police side) using the secret key. The secret key is calculated using the public components of the complainant (p,g,A) and police officer's security pin.The police officer takes further action.The blockchain used in this paper is Public Ethereum network which is based on proof of work concept.

Ethereum along with encryption provides transparency while also ensuring privacy of confidential data. The smart contract program which runs on the Ethereum blockchain creates an unalterable ledger and

makes sure that only those transactions that abide by the contract are committed to the network. The details of the complaint are encrypted by the procedure mentioned in the security module and the proofs provided by the user are stored on a public IPFS network. The transparent nature of Ethereum ensures that the presence of the complaint on the blockchain is visible to all the participants of the network. Further to maintain confidentiality the procedure explained in the security module is implemented. The hash corresponding to the proofs and encrypted complaint details is stored on the blockchain network. The police officer who is a participant in 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. Once the police FIR/NCR/Chargesheet, is rendered as a pdf and is encrypted using the similar procedure mentioned in the security module. This encrypted document is then stored on the IPFS network and the corresponding hash is stored on the Ethereum network.

IV. ALGORITHM

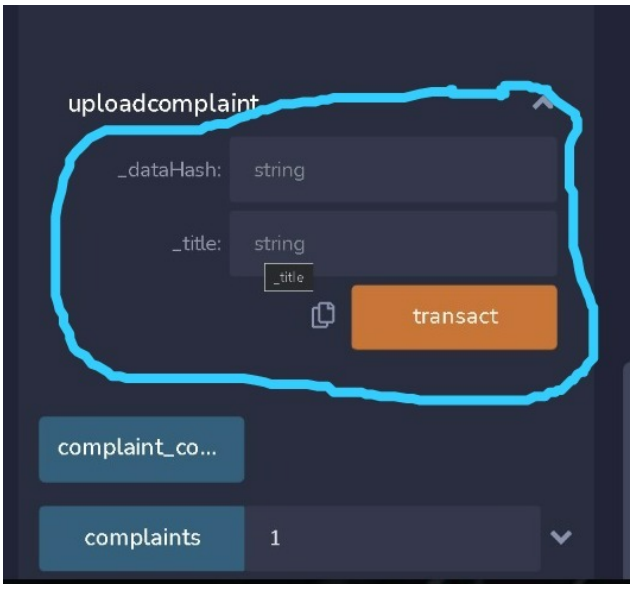
The algorithm steps of block generation and encryption strategies are as follows.

- **Step - 1** : Create an FIR file.
- **Step - 2** : The user attests the file with his/her cryptographic signature.
- **Step - 3** : Obtain pin, OTP verification further on.
- **Step - 4** : Then encrypt suspect name, victim name, and identification details of suspect and victim only, from labeled input-type form.
- **Step - 5** : The rest of the details are kept as it is.
- **Step - 6** : Block is generated.
- **Step - 7** : It is stored in IPFS.
- **Step - 8** : Hash is generated in IPFS.
- **Step - 9** : Along with Hash value, user name, unique id, and address is combined for smart contracts.
- **Step - 10** : Block is sent for mining (for now mining strategies are not explored).
- **Step - 11** : Assuming it is mined, The Decryption KEY is sent to concerned police authorities to carry out further investigation.
- **Step - 12** : After block mining, The hash is obtained.

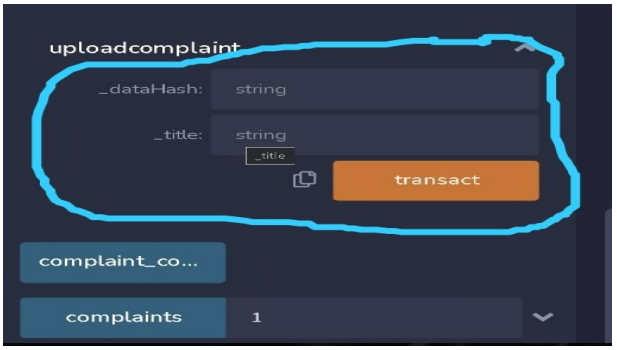
V. RESULTS

The algorithm has been designed to suit all the functionalities the authors aimed at achieving. The smart contract has developed and implemented and is up running. A basic level of Web Application has been designed though works remains to be in to enhance the user experience. It is a very positive sign looking at the stage the authors are in right now, in developing this project. A screenshot of the deployed smart contract is attached herein.

INPUT :



OUTPUT :



VI. CONCLUSION AND FUTURE SCOPE

Future is hopeful with blockchain technology. Infact future is already here. Things can be turned upside down with implementation of cutting edge technology in important sectors that are dying in the dire need of revamption. Now is the time. So many shortcomings can be overcomed is beyond imagination. And even with our current work many works still remain to be done.

The future scope is plentiful. Few listed below:

- Designing the algorithm of the mining procedure of the block after it is generated in a way that all target objectives are met.
- Enhancing user experience in the web application or the mobile application.
- Keep the scalability of the architecture intact with the increasing inflow of users.

VII. REFERENCES

1. Hingorani, Ishwarlal & Khara, Rushabh & Pomendkar, Deepika & Raul, Nataasha. (2020). Police Complaint Management System using Blockchain Technology. 1214-1219. 10.1109/ICISS49785.2020.9315884.

2. Arnab Mukherjee and Raju Halder. 2020. PoliceChain: Blockchain-Based Smart Policing System for Smart Cities. In 13th International Conference on Security of Information and Networks (SIN 2020). Association for Computing Machinery, New York, NY, USA, Article6,1–5.DOI:https://doi.org/10.1145/3433174.3433618

3. Hassija, Vikas & Patel, Aarya & Chamola, Vinay. (2021). Police FIR Registration and Tracking Using Consortium Blockchain. 10.1007/978-981-15-5243-4_75.