BLOCKCHAIN-POWERED POLICE COMPLAINT MANAGEMENT SYSTEM FOR ENHANCED TRANSPARENCY

M Rakesh[1], Anjali Patlolla[2], Bala Nagesh Muthyala[2], Meghna Maska[2]

[1]Assistant Professor, [2]UG Scholar, [1,2]Department of Computer Science & Engineering.

[1,2]Kommuri Pratap Reddy Institute of Technology, Ghatkesar, Hyderabad, Telangana.

ABSTRACT

In recent years, technological advancements have ushered in transformative changes across various sectors, and the realm of law enforcement is no exception. The traditional police complaint management system typically relies on centralized databases and manual processes, making it susceptible to various vulnerabilities. Complaint records are stored in a centralized manner, leaving them susceptible to unauthorized alterations or data breaches. The lack of a transparent and auditable trail further complicates the resolution process, leading to delays and a lack of accountability. Inefficiencies in communication and coordination can exacerbate these challenges, leaving both the complainants and law enforcement agencies dissatisfied with the overall system. Therefore, the need for a robust and transparent police complaint management system is imperative in maintaining public trust and ensuring accountability within law enforcement agencies. Citizens and stakeholders demand a system that is not only efficient but also capable of preventing tampering and ensuring the integrity of complaint records. Addressing this need requires a technological solution that can overcome the limitations of conventional systems. One such groundbreaking innovation is the integration of blockchain technology into the police complaint management system. Blockchain, originally designed as a decentralized ledger for cryptocurrencies, has proven its potential to revolutionize traditional systems by offering enhanced transparency, security, and accountability. Hence, this research proposes a integration of blockchain technology into the police complaint management system holds immense significance for enhancing transparency and accountability. Blockchain, with its decentralized and tamper-resistant nature, ensures that complaint records are securely stored and cannot be altered without detection. Smart contracts can automate and streamline the resolution process, reducing delays and improving overall efficiency. Every transaction or update is recorded in a transparent and immutable ledger, providing an auditable trail for all stakeholders. This not only fosters trust between the public and law enforcement but also contributes to a more accountable and responsive justice system.

Keywords: Blockchain Technology, Decentralized Ledger, Ethereum, Tokenization

1. INTRODUCTION

In India, allegations of violations must be officially recorded in accordance with the law. There are two categories of offenses, namely cognizable and non-cognizable offenses [3]. Cognizable offenses encompass grave criminal acts such as homicide, larceny, abduction, and sexual assault, among others. According to Section 2 (c) of the Criminal Procedure Code 1973, in the event of a cognizable offense, the police have the authority to apprehend the suspect without requiring a warrant [6]. The designated inspector may initiate the inquiry process autonomously, without requiring any directives from the court. When any recognizable crime is committed, a First Information Report (FIR) is filed at the police station. Any person, whether a victim or a witness to the incident, has the right to lodge a First Information Report (FIR). A First Information Report (FIR) contains essential

information such as the complainant's name and address, the date and time of the occurrence, the location, and a description of the facts surrounding the incident. After the registration of the FIR, the police officer proceeds to prepare a chargesheet report. The individual making the complaint can request the chargesheet by sending a letter under the Right to Information Act (RTI) and paying a certain fee to the court.

Non-cognizable offenses encompass illegal acts such as deception or forgery, among others. A non-cognizable complaint, also known as an N.C. complaint, can be filed at the police station. It exhibits a structure akin to that of a Finite Impulse Response (FIR) system. According to Section 2(l) of the Criminal Procedure Code of 1973, in the event of a non-cognizable offense, a police officer is not empowered to make an arrest or conduct an investigation without a warrant [6]. Prior to commencing the investigative process, the police officer must secure authorization from the court or judge. The crime rate, namely the number of crimes per one hundred thousand people, is escalating rapidly. A total of almost 5 million cognizable crimes were recorded in 2018 [1]. Owing to escalating criminal activities and the prevalence of corrupt law enforcement officers, they often decline, evade, or detain the process of registering First Information Reports (FIRs), Non-Cognizable Reports (NCRs), or complaints. These actions serve as hindrances for the individuals filing the complaints, impeding their ability to seek justice from the outset. Based on a poll [2], 24% of individuals encountered difficulties in registering their complaints, with 9% attributing the non-registration to being coerced into paying a bribe. Out of the individuals who were able to formally register their grievances, 30% of them did not receive a copy of the First Information Report (FIR). There is a requirement for an open and accountable system to eliminate corruption from the public systems.

Our objective is to introduce a blockchain-based online system for managing First Information Reports (FIRs) and Non-Cognizable Reports (NCRs) in a decentralized way. This system aims to address issues when police personnel refuse to register complaints. Blockchain technology utilizes a peer-to-peer network topology, meaning it is a distributed and decentralized data structure that stores all valid transactions in interconnected blocks. The initial implementation of blockchain technology is exemplified by bitcoin [5], a concept introduced by Satoshi Nakamoto. The primary purpose of blockchain is to ensure that only legitimate blocks are added to the chain, meaning that a block must obtain a minimum number of votes or consensus. Block validation is achieved by consensus procedures like as Proof of Work, Proof of Stake, and Proof of Capacity. Once a block of transactions is added to the network, it becomes computationally infeasible to tamper with the block. The Interplanetary File System (IPFS) is an algorithm that utilizes a peer-to-peer network to store and distribute files in a decentralized manner. The technique employs content-based addressing, meaning that each file is hashed (depending on its content) and stored in a decentralized network. By integrating IPFS with blockchain, it is possible to enhance the system with attributes such as immutability, exceptional dependability, and increased throughput. In this particular context, we offer a decentralized application that monitors all the activity associated with police complaints, starting from the filing of a complaint to the submission of a charge-sheet to the court. Blockchain technology guarantees confidence between the complainants and the police department. The system is not only impervious to data loss, but also resistant to brute force hacking and other forms of harmful attacks.

2. LITERATURE SURVEY

In [7], authors presented a robust and protected solution for FIR (First Information Report) utilizing blockchain technology. The proposed approach obviates the necessity for reliance on

the police by the general people. The system consists of four key stakeholders: the complainant, witness, investigating officer, and the suspect. The decentralized system would empower the pertinent parties to monitor and safeguard the digital FIR against any misconduct, ensuring a comprehensive record of all activities.

The researchers in [8] presented an internet-based unified system for managing police complaints in Saudi Arabia. Any individual who has completed the registration process can submit a complaint using an online platform upon seeing any dubious behavior. The police will authenticate the information and, based on the complaint and proof presented, will officially record the complaint in the system. In addition, they have diligently preserved crime-related data to monitor the whereabouts of the most sought-after or prominent criminals in the nation.

Authors in [9] suggested the implementation of an E-Police System, where users may submit their complaints using an android application that is hosted on a WAMP server. Law enforcement personnel can utilize an online interface to retrieve and modify information pertaining to complaints. In addition, they have emphasized the numerous benefits of an E-police system compared to the traditional pen and paper-based FIR registration approach. IMEI numbers have been utilized for the purpose of distinct user identification.

In [10], the researchers presented a method that allows users to register FIR under the relevant parts of the Indian Penal Code (IPC) that are applicable to their complaint. Additionally, it explores a 'SOS' mechanism that can be employed by a user in the event of a dire situation. Under those circumstances, the user's position will be transmitted to the adjacent police station. Complaints through the Mobile app are restricted to authorized users only.

3. PROPOSED SYSTEM

This project implements a Django web application for managing a police system that aims to provide a secure and transparent system for managing police records, complaints, and investigations using blockchain and IPFS technologies. Below is an overview of the project's functionality and structure:

- Blockchain and Smart Contract Integration: The project interacts with an Ethereum blockchain and utilizes a smart contract named "Police" to store and retrieve data. The smart contract is defined in a JSON file ("Police.json").
- IPFS Integration: The application integrates with IPFS (InterPlanetary File System) for storing and retrieving files. IPFS is used to store data related to complaints and investigations securely.
- User Authentication: The project implements user authentication with separate login actions for police officers and administrators (admin).
- Data Storage and Retrieval: The smart contract handles the storage of various types of data, including user details, complaints, and investigation information. The Django application provides views to read and write data to the smart contract.
- File Handling and Encryption: The application supports the upload and download of files related to complaints. Files are encrypted using the AES encryption algorithm before being stored in IPFS.
- Key Generation

To overcome from the issue arisen in existing system, this work suggesting migrating such inventory to Blockchain based server where data storage is immutable which means data cannot be alter in any manner after storage. Blockchain is a decentralized network which store data in multiple nodes and if one node is down then it can retrieve data from other working nodes. Blockchain store each record as

block or transaction and associate each block with hash code and before storing any new block then it will verify hash code of each old blocks and if all records verified successfully then only it will store new records. So, data alteration is impossible in Blockchain.

To implement this project, we have designed following modules:

- Admin: admin can login to application using username and password as 'admin' and 'admin'. After login admin will add Police employees and then give username and password to each police personnel. Admin can view all added police personnel and can view all investigations reports.
- Police: police can login to application using username and password given by admin and then add new FIR and can add updated investigations and all other police station peoples can view all FIR and updated investigations.

All documents and images uploaded to Blockchain will get saved inside IPFS server as Blockchain designed to store simple transaction data not the document files. So, here IPFS is utilized to store the document and gives the document storage address as hashcode and this hashcode will get saved inside Blockchain and later Blockchain will use this hashcode to download the files. To store record in Blockchain we need to design SOLIDITY Smart Contract code and this code contains all functions to store farmer and staff details and then this contract will be deployed on Blockchain Ethereum tool. After deployment we can call this contract to read and store data by using PYTHON WEB3 package.

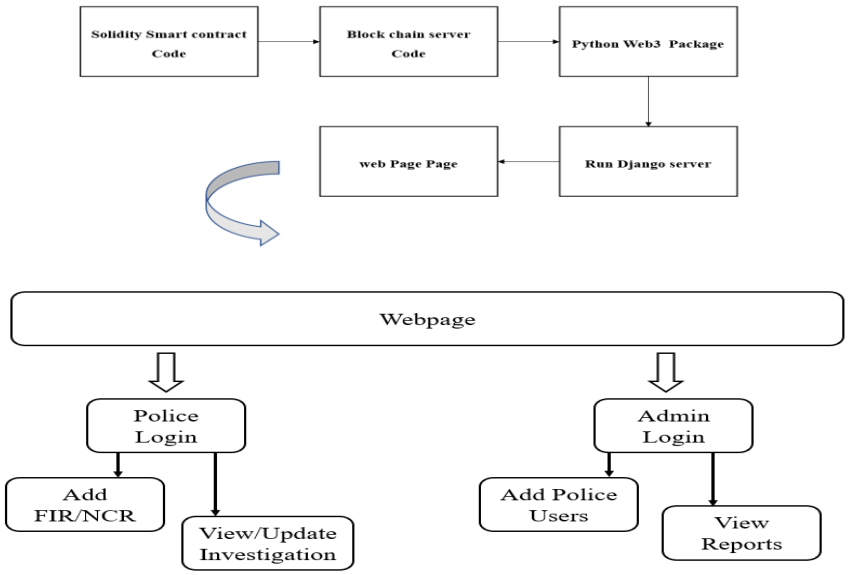


Figure 1: Overall architecture of proposed police complaint management system.

Ethereum

Ethereum is a decentralized blockchain platform that allows developers to build decentralized applications and execute smart contracts. It was launched in 2015 by Vitalik Buterin and quickly became one of the most popular blockchain platforms in the world, second only to Bitcoin in terms of market capitalization. Ethereum's main innovation is the ability to create smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. These smart contracts are executed on the Ethereum Virtual Machine (EVM), which is a decentralized, Turing-complete virtual machine that runs on the Ethereum network. The Ethereum network also has its own cryptocurrency called Ether (ETH), which is used to pay for transaction fees

and computational services on the network. ETH is also used as a store of value and traded on cryptocurrency exchanges. Overall, Ethereum provides a flexible platform for developers to build decentralized applications and execute complex smart contracts in a secure, transparent, and decentralized manner.

Advantages of Ethereum

Ethereum provides several advantages over other blockchain platforms and traditional systems. Here are some of the main advantages of Ethereum:

Smart Contracts: Ethereum's main innovation is the ability to create smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. This allows for secure and automated execution of complex agreements without the need for intermediaries or third parties.

Decentralization: Ethereum is a decentralized platform, which means that it is not controlled by any single entity or organization. This provides a level of trust and transparency, as there is no single point of failure or vulnerability.

Interoperability: Ethereum's blockchain is open-source and allows for interoperability with other blockchain platforms, making it easier to integrate with existing systems and applications.

Programmable: Ethereum's blockchain is programmable, which means that developers can create custom applications and smart contracts that meet their specific needs. This allows for more flexibility and customization than traditional systems.

Security: Ethereum's blockchain is secured through cryptographic algorithms and consensus mechanisms, making it resistant to hacking and fraud. Additionally, smart contracts on the platform are auditable and transparent, which helps to reduce the risk of fraud and corruption.

Tokenization: Ethereum enables the creation and exchange of tokens, which can represent assets, securities, or other digital assets. This makes it possible to create new business models and revenue streams that were previously not possible.

Overall, Ethereum provides a powerful and flexible platform for developers to build decentralized applications and execute complex smart contracts in a secure, transparent, and decentralized manner.

WEB3 Python Package

web3.py is a Python library that provides a simple and easy-to-use API for interacting with Ethereum networks using JSON-RPC. It allows developers to easily interact with smart contracts, send transactions, and access blockchain data.

Some of the key features of web3.py include:

Contract interaction: web3.py provides an API for interacting with smart contracts on the Ethereum network. This includes functions for deploying contracts, calling contract functions, and reading contract data.

Transaction management: web3.py makes it easy to send transactions to the Ethereum network, including specifying gas prices and gas limits.

Event listening: web3.py allows developers to listen for events emitted by smart contracts on the Ethereum network, making it easy to build real-time applications that react to blockchain data.

Blockchain data access: web3.py provides functions for accessing blockchain data like account balances, transaction history, and block data.

Integration with popular wallets: web3.py integrates with popular Ethereum wallets like Metamask and Geth, making it easy to manage accounts and interact with the network. Overall, web3.py is a powerful tool for building

decentralized applications on the Ethereum network using Python.

Blockchain

Blockchain is a decentralized, digital ledger technology that is used to record and store data in a secure and transparent manner. It is a distributed ledger, meaning that it is maintained by a network of computers, rather than being controlled by a single entity. Each block in the chain contains a set of transactions, and once a block is added to the chain, it cannot be altered or deleted. This makes blockchain an immutable and tamper-resistant technology that is particularly well-suited for storing and transmitting sensitive data.

Blockchain technology is perhaps best known for its use in cryptocurrencies like Bitcoin and Ethereum, but it has a wide range of other potential applications as well. These include supply chain management, identity verification, voting systems, and more. The decentralized nature of blockchain means that it has the potential to disrupt a variety of industries and business models by enabling trust and transparency in transactions and data exchange.

Concepts

There are several key concepts that are important to understand when it comes to blockchain technology:

Decentralization: Blockchain is a decentralized technology, meaning that it is not controlled by any single entity, but rather maintained by a network of participants. This increases transparency, security, and resilience.

Distributed ledger: Blockchain technology uses a distributed ledger to record and store data. Each block in the chain contains a set of transactions, and once a block is added to the chain, it cannot be altered or deleted.

Cryptography: Blockchain technology uses advanced cryptographic algorithms to secure transactions and data exchange, making it highly resistant to hacking and cyber attacks.

Consensus mechanism: In a blockchain network, participants must agree on the validity of transactions before they are recorded on the blockchain. Different blockchain networks use different consensus mechanisms to achieve this, such as Proof of Work or Proof of Stake.

Smart contracts: Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They can be used to automate complex transactions and ensure that all parties involved in a transaction adhere to the terms of the contract.

Tokenization: Blockchain technology enables the creation of digital tokens that can be used to represent a variety of assets, such as currencies, commodities, or even real estate.

Blockchain technology has a wide range of potential applications across various industries. Some examples of how blockchain is currently being used, or has the potential to be used, include:

Cryptocurrencies: Blockchain technology is the foundation of cryptocurrencies like Bitcoin and Ethereum, which use blockchain to enable peer-to-peer transactions without the need for a centralized intermediary.

Supply chain management: Blockchain technology can be used to create transparent and secure supply chain systems, allowing participants to track and verify the origin and authenticity of products.

Identity verification: Blockchain technology can be used to create secure and tamper-proof digital identity systems, allowing individuals to prove their identity without the need for a centralized authority.

Voting systems: Blockchain technology can be used to create secure and transparent voting systems, ensuring the accuracy and legitimacy of election results.

Healthcare: Blockchain technology can be used to create secure and transparent healthcare

systems, enabling secure sharing of patient data and facilitating drug traceability.

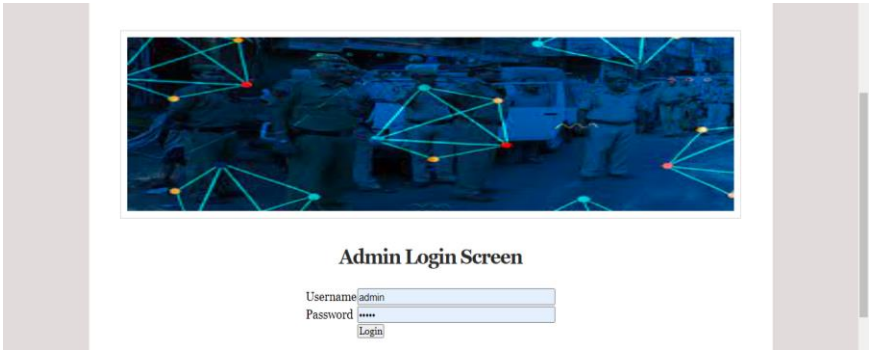
Finance: Blockchain technology can be used to create more efficient and secure financial systems, allowing for faster and cheaper transactions while reducing the risk of fraud and corruption.

Real estate: Blockchain technology can be used to create more transparent and secure real estate transactions, allowing for faster and more efficient transfer of ownership.

These are just a few examples of how blockchain technology is being used, and there are many other potential applications that are currently being explored.

4. RESULTS

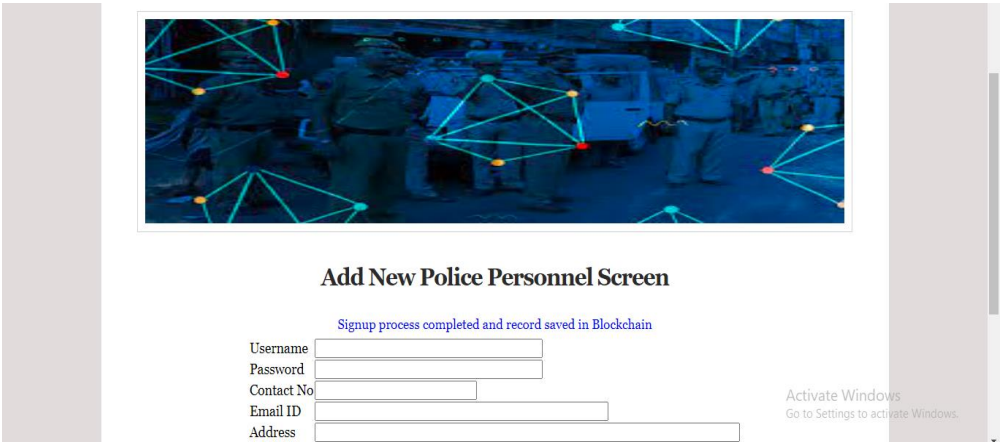
In below screen click on 'Admin Login' link to get below login screen



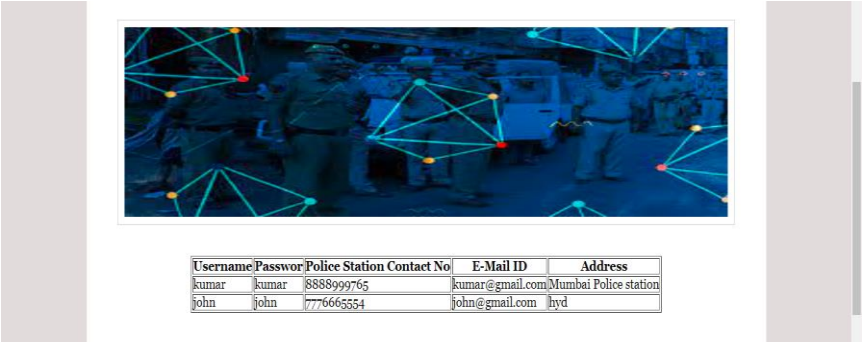
In above screen admin is login and after login will get below page.

In above screen admin can click on 'Add New Police Users' link to get below page.

In above screen admin will add new Police personnel details and then give this login details to police personnel to add FIR details.

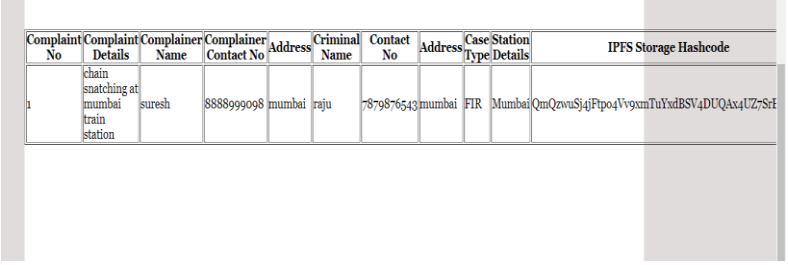


In above screen police details added in Blockchain and now click on 'View Police Personnel' link to view all available police men details.

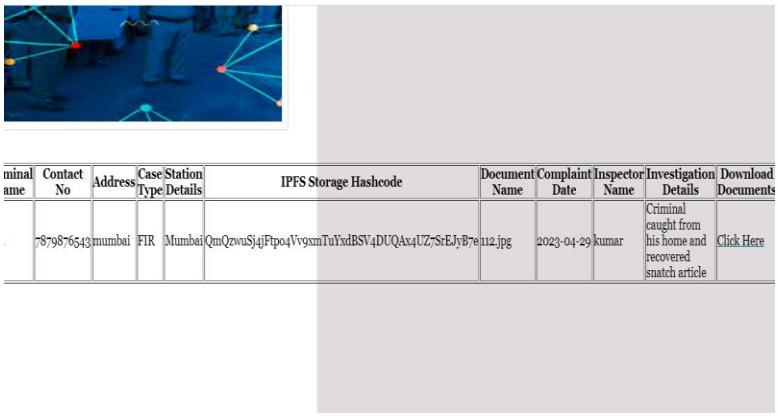


Username	Passwor	Police Station Contact No	E-Mail ID	Address
kumar	kumar	8888999765	kumar@gmail.com	Mumbai Police station
john	john	7776665554	john@gmail.com	hyd

In above screen admin can view all police details and now click on 'View Reports' link to view all existing FIR reports and investigations.

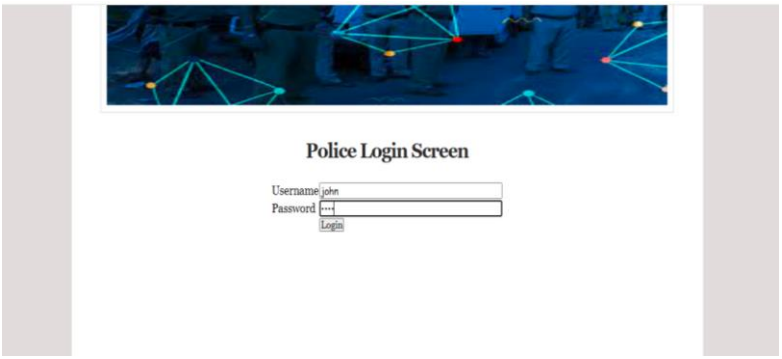


Complaint No	Complaint Details	Complainer Name	Complainer Contact No	Address	Criminal Name	Contact No	Address	Case Type	Station Details	IPFS Storage Hashcode
1	chain snatching at mumbai train station	suresh	8888999098	mumbai	raju	7879876543	mumbai	FIR	Mumbai	QmQzwuSj4jFtpo4Vv9xmTuYxdBSV4DUQAx4UZ7SrE



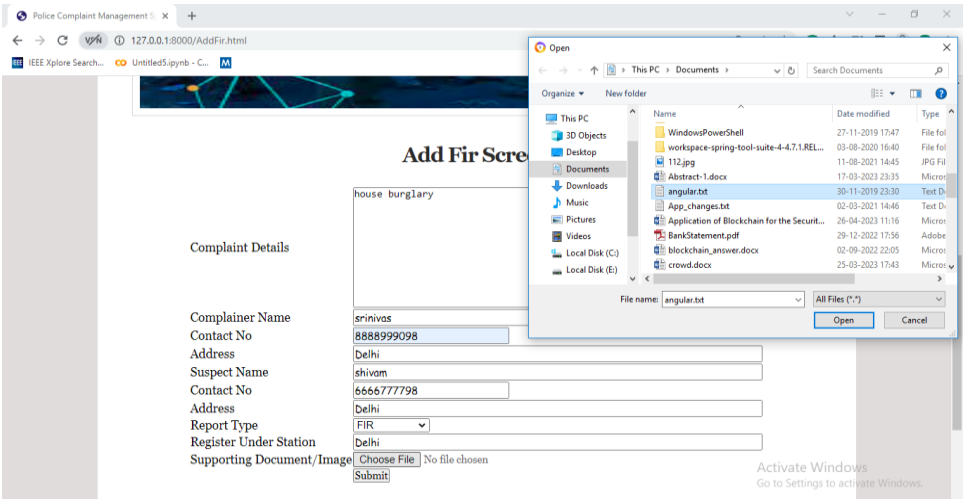
minal ame	Contact No	Address	Case Type	Station Details	IPFS Storage Hashcode	Document Name	Complaint Date	Inspector Name	Investigation Details	Download Documents
	7879876543	mumbai	FIR	Mumbai	QmQzwuSj4jFtpo4Vv9xmTuYxdBSV4DUQAx4UZ7SrEJyB7e	112.jpg	2023-04-29	kumar	Criminal caught from his home and recovered snatch article	Click Here

In above two screen admin can view all previously added FIR reports and can click on 'Click Here' link to download all crime related report and this report will be saved in Blockchain in encrypted format. Now logout and login as Police personnel.



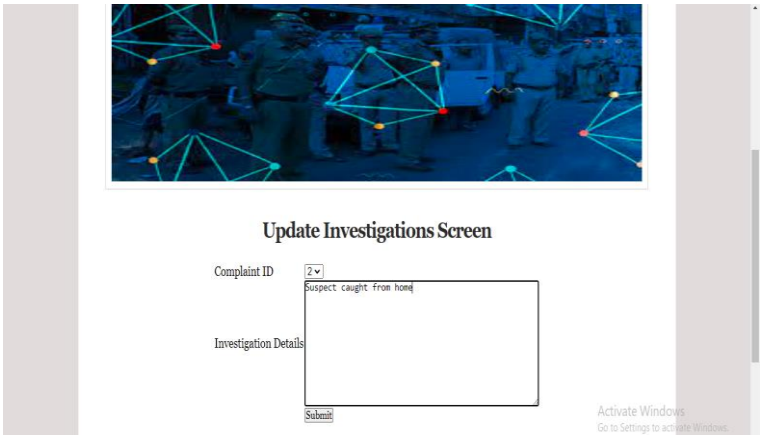
In above screen police personnel is login and after login will get below page

In above screen police can click on 'Add FIR/NCR/Charge sheet' link to add FIR

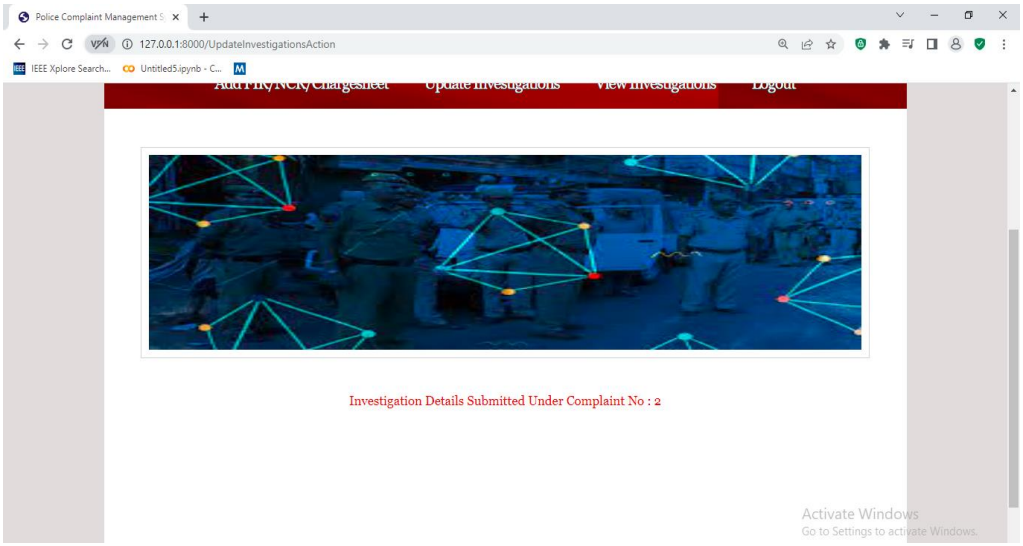


In above screen police user can add all Crime details as FIR and then upload crime related file and then click on 'Open' and 'Submit' button to get below output

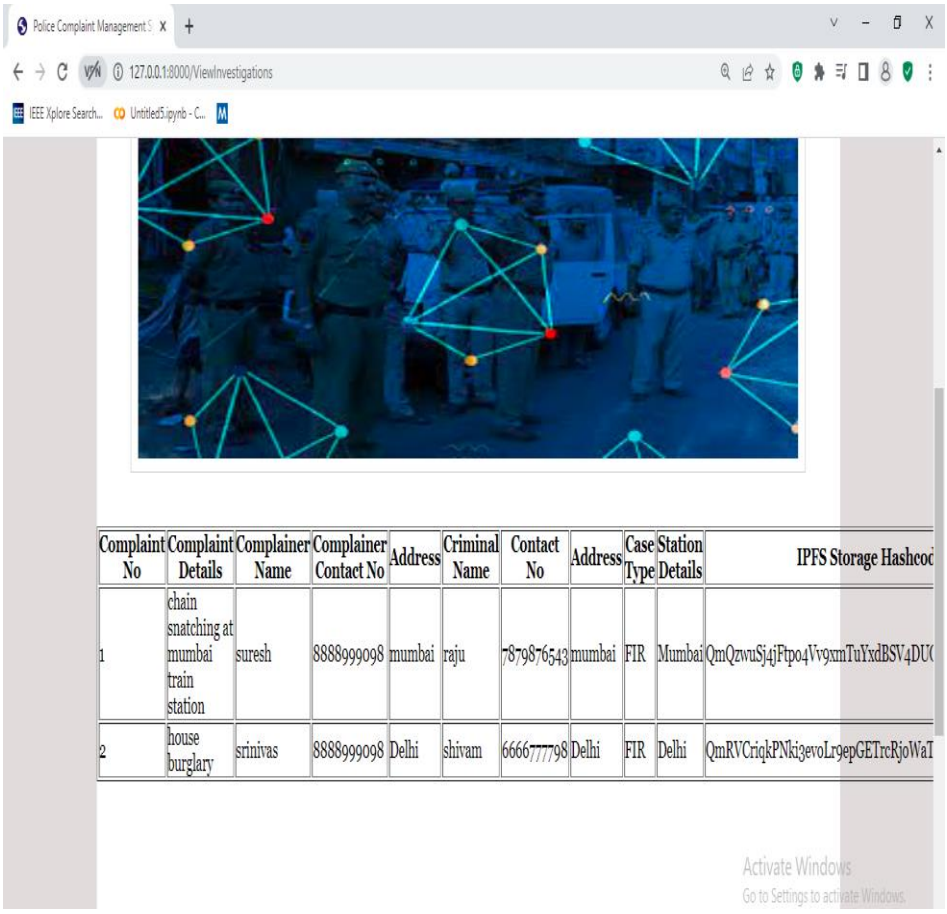
In above screen complaints details added to Blockchain and file get saved in IPFS and now police can click on 'Update Investigation' link to add future investigation data to current FIR like below page



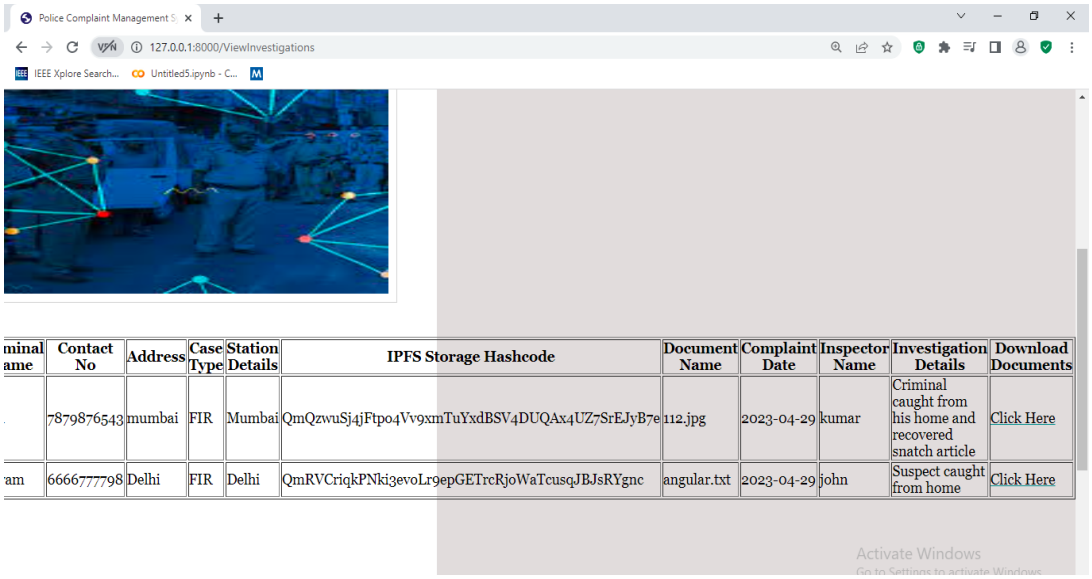
In above screen police will select complaint number and then add investigation data and then press button to save data in Blockchain and then will get below page



In above screen we can see investigation details updated and now click on 'View Investigation' link to get below investigated and complaint details from Blockchain



Complaint No	Complaint Details	Complainer Name	Complainer Contact No	Address	Criminal Name	Contact No	Address	Case Type	Station Details	IPFS Storage Hashcod
1	chain snatching at mumbai train station	suresh	8888999098	mumbai	raju	787987654 3	mumbai	FIR	Mumbai	QmQzwuSj4jFtpo4Vv9xmTuYxdBSV4DU(
2	house burglary	srinivas	8888999098	Delhi	shivam	6666777798	Delhi	FIR	Delhi	QmRVCriqkPNki3evoLr9epGETrcRjoWaI



minal ame	Contact No	Address	Case Type	Station Details	IPFS Storage Hashcode	Document Name	Complaint Date	Inspector Name	Investigation Details	Download Documents
	7879876543	mumbai	FIR	Mumbai	QmQzwuSj4jFtpo4Vv9xmTuYxdBSV4DUQAx4UZ7SrEJyB7e	112.jpg	2023-04-29	kumar	Criminal caught from his home and recovered snatch article	Click Here
am	6666777798	Delhi	FIR	Delhi	QmRVCriqkPNki3evoLr9epGETrcRjoWaTcusqJBJsRYgnc	angular.txt	2023-04-29	john	Suspect caught from home	Click Here

In above screen police can view all crime investigation from Blockchain from anywhere.

5. CONCLUSION

The presented project, a comprehensive police management system leveraging blockchain and IPFS technologies, demonstrates a robust and secure solution for handling police records, complaints, and investigations. The integration of Ethereum blockchain ensures data integrity, transparency, and tamper resistance, while IPFS serves as a reliable and decentralized file storage system. The use of Django as the web framework facilitates seamless interactions between users, police officers, and administrators, providing a user-friendly interface for various actions. The project's encryption mechanisms, employing AES for file encryption and PBKDF2 for key generation, enhance the security of sensitive information. The web application supports functionalities such as submitting complaints, managing investigations, and viewing reports, catering to both police officers and administrators. The incorporation of IPFS for file storage adds an additional layer of security and decentralization.

REFERENCES

[1] https://ncrb.gov.in/sites/default/files/Crime%20in%20India%202018%20-%20Volume%201.pdf

[2] https://www.tatatrusts.org/upload/pdf/spir-2018-common-cause.pdf

[3]http://epgp.inflibnet.ac.in/epgpdata/uploads/epgpcontent/S001608/P001746/M022182/ET/1504501511Module-21-Q1.pdf

[4] http://www.thanepolice.gov.in/faq14.php

[5] https://bitcoin.org/bitcoin.pdf

[6] https://indiankanoon.org/doc/760919/

[7] 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

[8] 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.

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

[10] 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).