Tec Empresarial
P-ISSN: 1659-2395; E-ISSN: 1659-3359

PUBLIC OBJECTION BY CRIMINAL TO POLICE HEADQUARTERS SHORT A WAY SET CASUALTY

Pavitraa.D.S.B
Department of Information Technology, Panimalar Engineering College, India

Kaarthika.N
Department of Information Technology, Panimalar Engineering College, India

Sangeetha.G
Department of Information Technology, Panimalar Engineering College, India

Mrs.V.Priyadharshini
Assistant professor
Department of Information Technology, Panimalar Engineering College, India

ABSTRACT:

This project aims to address the public objection process in criminal cases by providing a secure and efficient system utilizing Java programming language and the SHA-256 algorithm of the blockchain. The system includes a login and registration page for users, as well as modules for the police headquarters and the admin. The system ensures the authenticity and integrity of objection submissions by leveraging the blockchain's decentralized and immutable nature. The SHA-256 algorithm provides a robust cryptographic mechanism for securing data and maintaining the integrity of the objection records. The login and registration page allows users to securely access the system and submit their objections to the police headquarters. The system incorporates modules specifically designed for the police headquarters and the admin to handle and process the objections efficiently. By utilizing blockchain technology, the system ensures transparency and accountability throughout the objection process. Each objection submission is recorded on the blockchain, making it tamper-proof and verifiable. This enhances trust between the public and the police authorities, as well as streamlines the objection-handling process.

I.INTRODUCTION:

In the realm of criminal justice systems, the efficient and transparent handling of public objections is crucial to maintaining trust and accountability. This project endeavors to revolutionize the objection process in criminal cases by introducing a secure and streamlined system, employing the Java programming language and the robust SHA-256 algorithm of the blockchain. Through the utilization of blockchain technology, the system aims to address public concerns by ensuring the authenticity, integrity, and transparency of objection submissions. The core architecture of the system encompasses a user-friendly login and registration interface, facilitating secure access for users keen on submitting objections. Designed with a focus on enhancing user experience, this aspect of the system is pivotal in establishing a secure connection between the public and the criminal justice framework. One of the key features of this project is its incorporation of modules tailored for both the police headquarters and the admin. These specialized modules are crafted to efficiently handle and process objections, thereby optimizing the overall workflow within the criminal justice framework. The blockchain's decentralized and immutable nature adds an extra layer of security, assuring the integrity of objection records

The main goal of this initiative is to create a secure, transparent, and efficient complaint registration system. The system aims to offer users a smooth experience for submitting their complaints by gathering essential details like complaint description, category, and date of occurrence. Additionally, users will have the capability to track the status of their complaints from pending to resolved, ensuring they stay informed about the progress of their issues. To guarantee the security and integrity of the data, the system will employ blockchain technology. This technology ensures that the complaint data remains tamper-proof and only the designated complaint registration wallet can update the complaint status, bolstering the overall security of the system. Transparency is another key objective of this initiative.

II.LITERATURE SURVEY

[1]Ishwarlal Hingorani, Rushabh Khara, Deepika Pomendkar, and Nataasha Raul 2020 proposed a police complaint management system that utilizes blockchain technology for enhanced registration, tracking, and management of complaints. The system addresses the bottleneck issue by implementing a public blockchain system where transactions are broadcast to every node. It employs a 16-bit AES encryption algorithm to secure the details and utilizes the Diffie Hellman key exchange technique for exchanging secret keys. The system includes user-side and police-side interfaces distributed via web and mobile interfaces. It aims to create a decentralized platform by leveraging technologies like blockchain and IPFS for processing complaints securely and efficiently.

[2] The E-Police System outlined in this study comprises an Android mobile application and a dedicated website tailored for police department use. This approach addresses two distinct types of complaints and involves the complainant, who initiates the process by filling out the FIR form. The complainant has the authority to upload diverse materials, such as images, audio files, and videos. Police officers can then access these records through an online portal, where they verify the information and conduct further investigations.

[3] The described Blockchain Criminal Record Management System (CRAB), as detailed in this paper, introduces a criminal record storage approach utilizing blockchain technology to enhance integrity and security. It addresses the challenge of separate databases within government law enforcement institutions hindering seamless information transfer by adopting cloud storage. To ensure proof of material integrity during court proceedings, the transaction log and provenance data are stored on the blockchain. The system employs Elliptic Curve Cryptography (ECC) encryption to safeguard illegal data. Furthermore, a Smart Provenance system is implemented on

the Ethereum platform, utilizing smart contracts for file information storage and event log preservation.

[4] A Simple Implementation of Criminal Investigation using Call Data Records (CDRs) through Big Data Technology. In this investigation, call data records (CDRs) from both suspects and victims are analyzed, employing Hive for data summarization and Hadoop for processing and storing extensive CDR datasets. The resulting system-generated report not only identifies frequently called users and those with prolonged call durations but also provides valuable assistance to authorities in future investigations. The detection of callers with rapidly changing IMEI numbers is flagged as potentially suspicious conduct. The anti-crime team seamlessly integrates evidence evaluations with insights from the report. The utilization of TreeMap in Java maintains order, while the MapReduce algorithm calculates frequent callers, stored as key-value pairs to ensure uniqueness. This innovative approach transforms raw data into an effective tool for streamlining criminal investigations.

[5] The primary goal of the Online FIR Filing System is to introduce an Android application that enables train passengers to report crimes by filing an FIR, specifically addressing incidents occurring on trains. In emergencies, Government Railway Police (GRP) officials can promptly access the FIR to assist individuals. This application brings benefits to both the government railway police and passengers, maintaining an up-to-date victim database for future analysis. The system comprises a web portal for the police department and a user-friendly front end with public and admin portals—the latter being under government control. Prioritizing the security of user data, the system aims to provide swift services to travelers and facilitate effective police investigations, ultimately contributing to the reduction of crimes.

III.EXISTING SYSTEM

The study involves utilizing personal information and GPS trajectories to extract features, with a focus on representing individuals and locations as nodes in a network. The objective is to classify crime risks based on these features, creating a Multi-dimension Fusion Information Graph (FIG) that incorporates data from various sources. The proposed FIGAT model, which is built on graph neural networks, effectively addresses the limitations of existing studies that overlook individual GPS trajectory data when inferring crime locations or groups. These studies fail to consider the joint influence on crime patterns arising from the internal relationships among criminals, locations, and time.

In contrast, our research presents Fusion Information Graph Attention Networks (FIGAT) with the objective of categorizing individuals into high and low-risk groups through the analysis of personal movement time series and location trajectories. Addressing challenges related to independent crime behavior and information fusion loss, FIGAT introduces a Multi-dimension Fusion Information Graph, which amalgamates semantic correlation features with traditional individual basic features, time features, and location features. Employing a multi-relation graph attention layer, FIGAT utilizes semantic relationships and node information to accurately classify individuals into high and low-risk categories. The evaluation of FIGAT encompasses the analysis of 14,625,884 GPS trajectories from 1038 individuals, collected by a real-world public safety department.

Disadvantage :

Reliance on Personal Information and GPS Trajectories: FIGAT heavily relies on personal information and GPS trajectories for crime risk classification.

This dependence may limit its effectiveness if the data quality is compromised or if individuals provide inaccurate or incomplete information.

IV. PROPOSED SYSTEM

This project introduces a Java-based system for public objections in criminal cases, leveraging the SHA-256 algorithm of blockchain technology. The system includes login and registration pages, as well as modules for police headquarters and admin functions. By utilizing blockchain's decentralized and immutable nature, the system ensures secure objection submissions and maintains data integrity.It also has QR code verification for security purpose to sharing the files.

Advantage:

Robust Cryptographic Security: SHA-256 offers strong cryptographic security, making it highly resistant to hacking and unauthorized access.

Its 256-bit hash function provides a high level of data integrity and protection against tampering.

V.TECHNIQUES

SQL operations, SHA-256 (Secure Hash Algorithm 256-bit), and the Advanced Encryption Standard (AES) algorithm are essential elements in the fields of database management and cryptography, each with separate but related functions. Symmetric encryption technology AES is well known for having strong security features. It is used to encrypt sensitive data, guaranteeing confidentiality in communication and storage systems, and it works with fixed-size blocks of data. In contrast, SHA-256 functions as a cryptographic hash algorithm, processing any input data to produce a consistent, fixed-size (256-bit) output. Its primary role is to uphold data authenticity and integrity. Widely employed in digital signatures and certificate creation, SHA-256 ensures that each distinct input results in a unique hash value, practically eliminating the possibility of two different inputs producing the same hash. This attribute is crucial for verifying data accuracy and detecting any alterations or manipulation.

The well-known cryptographic standards AES (Advanced Encryption Standard) and SHA (Secure Hash Algorithm) perform encryption and hashing tasks more effectively than the resource-intensive nature of a complete blockchain implementation. Symmetric encryption algorithms like AES are known for their speed and adaptability in protecting data both in transit and in storage. Its efficiency comes from its capacity to handle massive amounts of data quickly while upholding strict security standards. Data integrity is ensured by SHA, especially SHA-256, a hashing algorithm that quickly generates a fixed-size hash result by creating unique identifiers for different inputs.

AES and SHA provide a more efficient method for completing particular cryptographic tasks than the extensive and resource-demanding nature of a full blockchain, which includes distributed consensus mechanisms and intricate validation procedures. While SHA guarantees dependable and speedy hashing, AES offers quick and efficient encryption. This efficiency is especially useful in situations when a full blockchain would not be required, which would require a lot of computing power and infrastructure. AES and SHA are frequently used in applications including data verification, authentication, and secure communications because of their reliability and security.

In conclusion, AES and SHA are better options for a range of cryptographic applications due to their superior performance in hashing and encryption. They are ideally suited for activities where a lean and efficient approach is required over the more complex and resource-intensive nature of a full blockchain implementation because of their speed and dependability.

AES ENCRYPTION

One of the simplest cybersecurity techniques is encryption, which may be used to protect sensitive data even in the event that the network it is on has been compromised. In straightforward terms, encryption transforms plain text into a code that only someone with the corresponding cipher or key can decode back into its original form.

The entire message is encrypted using the cipher in older symmetric encryption techniques. Nevertheless, the message is divided into smaller blocks by the AES algorithm. Moreover, there are multiple encryption transposition, and mixing—instead of just one.

Ten encryption rounds are applied to a 128-bit key, twelve to a 192-bit key, and fourteen to a 256-bit key. According to Mike Pedrick, vice president of cybersecurity consultancy at Nuspire, the outcome is practically difficult to break using a brute-force attack on modern machines. According to him, future quantum computing techniques might be able to break AES.

The AES algorithm consists of 4 phases in each round:

- Substitution: The process involves replacing plain text with encrypted text using a predetermined cipher.
- Shifting: Each row undergoes a one-position shift, with the exception of the first.
- Mixing: To prevent straightforward decryption by row shifting, the Hill cipher is applied to mix the columns.
- Additional Encryption: A fraction of the encryption key is utilized to encrypt the specific data block.

SHA-256

Secure Hashing Technique involves the utilization of a cryptographic hash function known as SHA-256, or 256-bit, which can convert any text into an almost unique 256-bit alphanumeric string. The resulting output is commonly referred to as a hash or hash value.

SHA-256 is a cryptographic security algorithm. Because this hashing technique generates unique, irreversible hash values, it is regarded as being incredibly secure.

The SHA-256 (NSA), part of the SHA-2 hash function family, was developed by the United States Government's National Security Agency (NSA), which has gained popularity after the The National Security Agency (NSA) recommended that U.S. federal entities transition from its forerunner, SHA-1, due to identified vulnerabilities in the hash function.

SHA-256 in Blockchain Technology

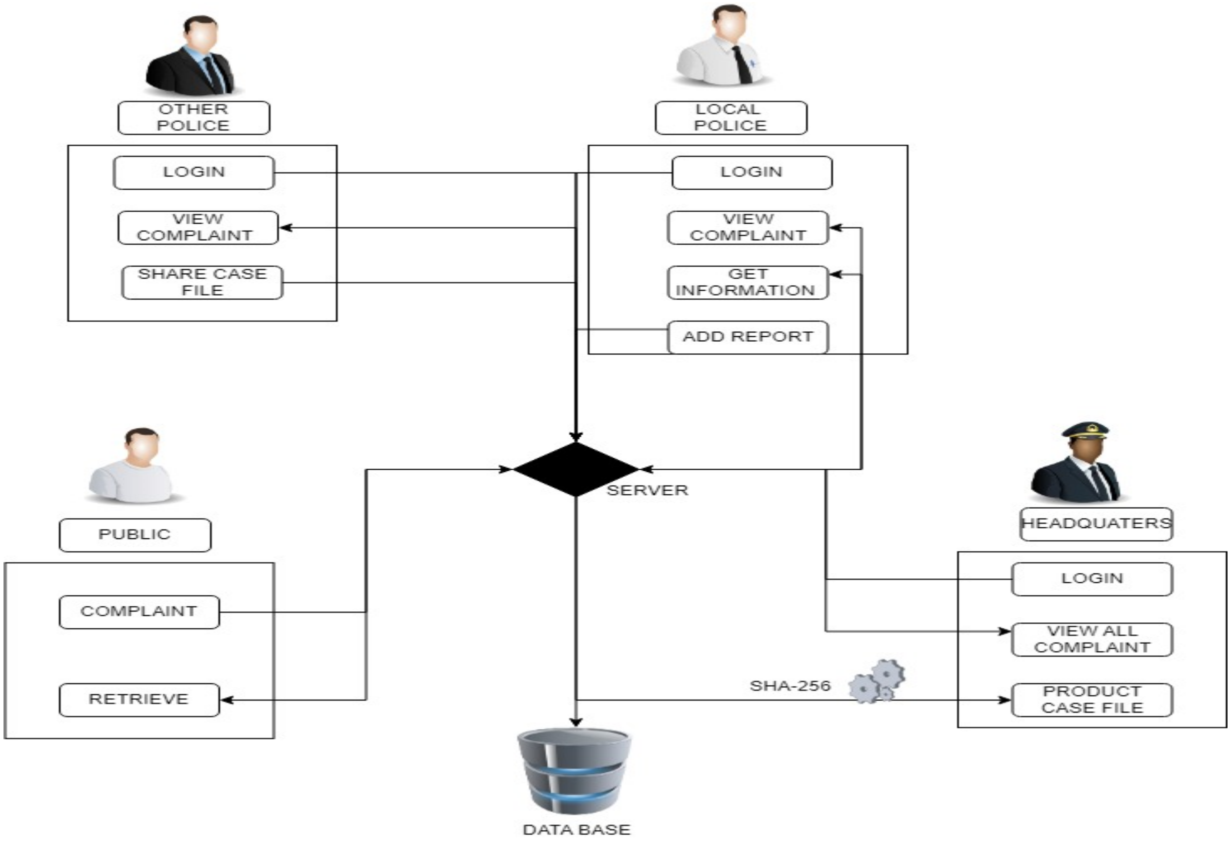
The SHA-256 hashing algorithm is used by PoW blockchains, such as Bitcoin, to validate transactions, build new blocks, and maintain the blockchain's security against attacks.

Proof-of-Work (PoW) mining utilizes the SHA-256 hash algorithm. When a new block is appended to the Proof-of-Work blockchain, a block hash is created. Miners are required to insert a random string of numbers, referred to as the nonce, into the data from the preceding block. They then process it through the SHA-256 algorithm to obtain the hash for the new block.

Guessing and checking is the only method to accomplish this.

The blockchain is protected against assaults by the massive computational effort needed to predict the proper string of integers that yields the correct SHA-256 hash values.

BLOCK DIAGRAM



I.MODULES:

PUBLIC:

In this application public doesn't need any register and login process. They are straightforwardly moved forward to the public home page and can use all features.

LOCAL POLICE:

Local police need to enter a username and secret word to open their landing page after that they can see all grumblings

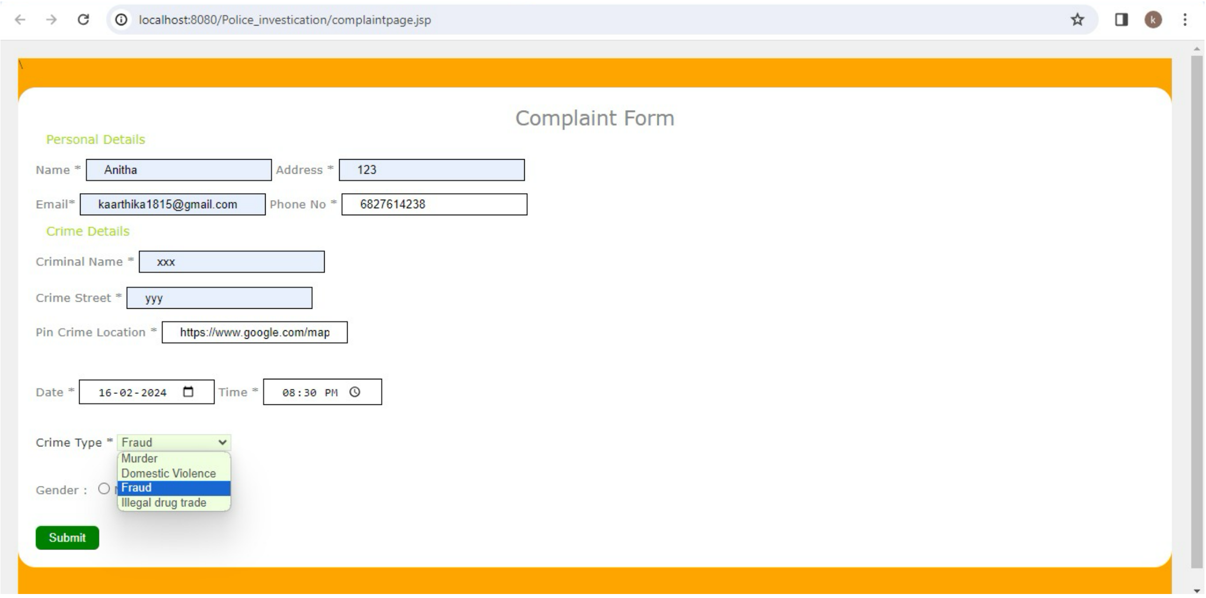
OTHER POLICE STATION:

Nearby police need to enter a username and secret word to open their greeting page after that they can see all grumblings and contrast with their data set assuming any case record matches that case they quickly send that case report to the neighborhood police station.

POLICE HEADQUARTERS:
Headquarters is one of the models of this application it has a secret username and secret phrase to open their point of arrival. It will keep the Case records securely.

PUBLIC COMPLAINT ABOUT CRIME:
If the public wants to make a complaint about a crime they should fill out the complaint form. That complaint form contains a few input tags. the public has to enter personal details and crime details.

LOCAL POLICE UPLOAD REPORT:
Nearby police need to enter the username and secret phrase to open their point of arrival and afterward if get any data from different stations make the prompt move and report to**VII.OUTPUT**



localhost:8080/Police_investication/complaintpage.jsp

Complaint Form

Personal Details

Name * Anitha Address * 123

Email* kaarthika1815@gmail.com Phone No * 6827614238

Crime Details

Criminal Name * xxx

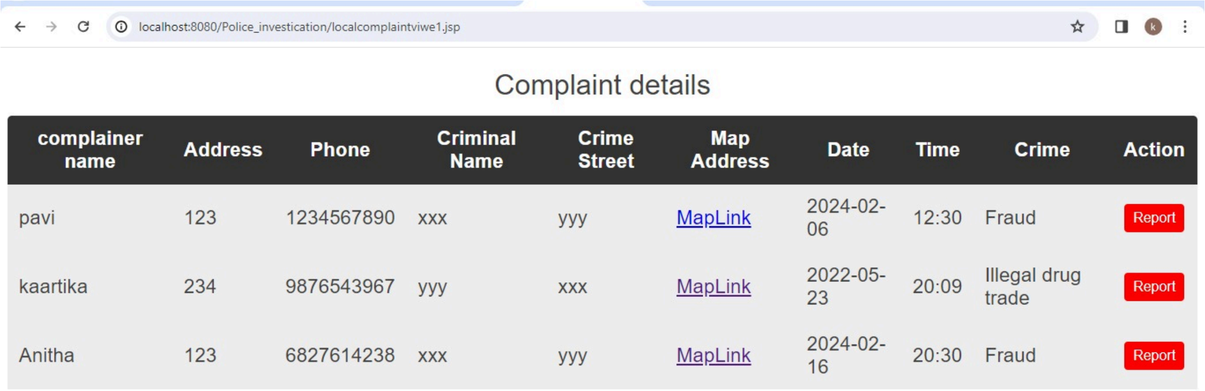
Crime Street * yyy

Pin Crime Location * https://www.google.com/map

Date * 16-02-2024 Time * 08:30 PM

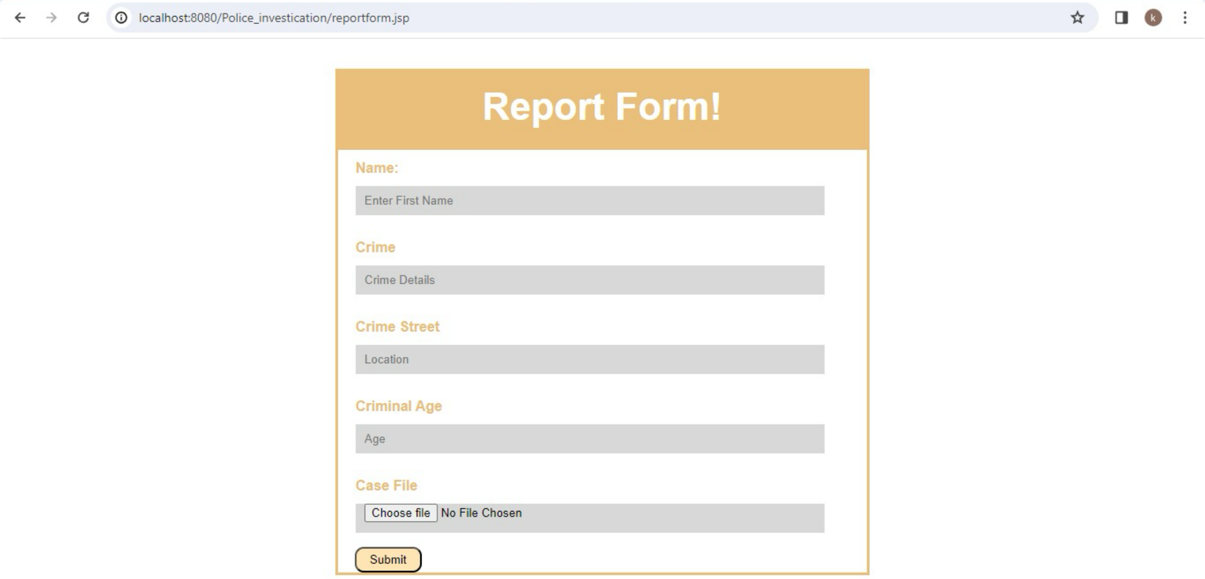
Crime Type * Fraud

Gender : ○



Complaint details

complainer name	Address	Phone	Criminal Name	Crime Street	Map Address	Date	Time	Crime	Action
pavi	123	1234567890	xxx	yyy	MapLink	2024-02-06	12:30	Fraud	Report
kaartika	234	9876543967	yyy	xxx	MapLink	2022-05-23	20:09	Illegal drug trade	Report
Anitha	123	6827614238	xxx	yyy	MapLink	2024-02-16	20:30	Fraud	Report



Report Form!

Name:

Enter First Name

Crime

Crime Details

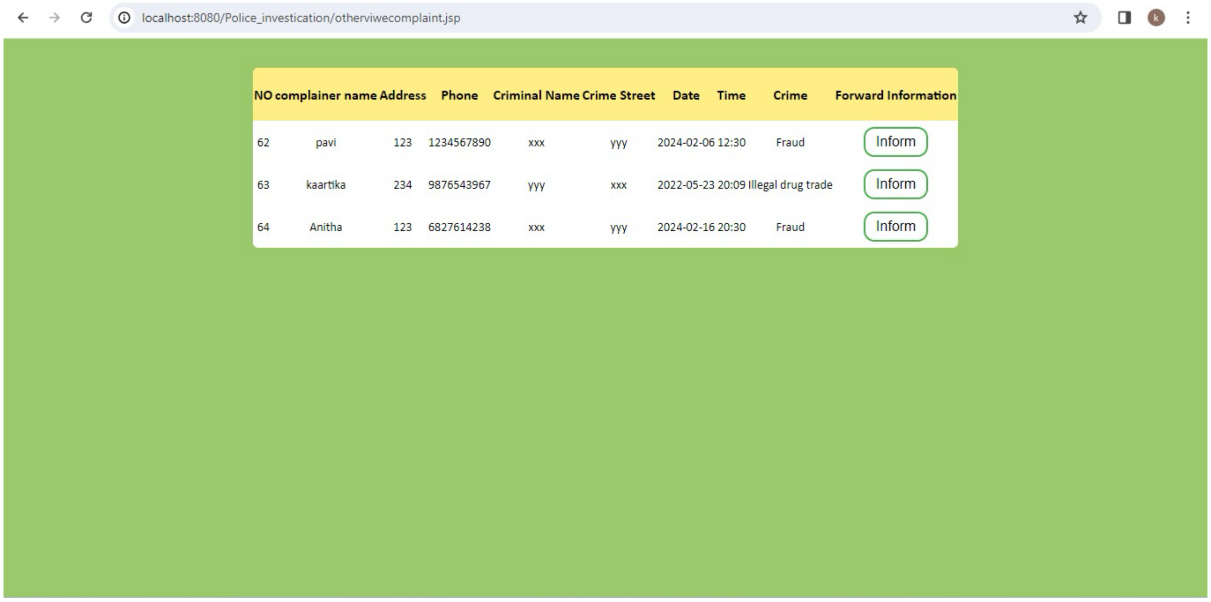
Crime Street

Location

Criminal Age

Age

Case File



NO	complainer name	Address	Phone	Criminal Name	Crime Street	Date	Time	Crime	Forward Information
62	pavi	123	1234567890	xxx	yyy	2024-02-06	12:30	Fraud	Inform
63	kaartika	234	9876543967	yyy	xxx	2022-05-23	20:09	Illegal drug trade	Inform
64	Anitha	123	6827614238	xxx	yyy	2024-02-16	20:30	Fraud	Inform

VIII. FUTURE ENHANCEMENTS:

Development of a practical database system.

Optimization of protocols for efficiency in terms of message exchange quantity and size.

Implement using two are more algorithms.

IX. CONCLUSION:

This project presents a comprehensive solution to streamline and enhance the public objection process in criminal cases. By leveraging the Java programming language, the SHA-256 algorithm, and blockchain technology, the system establishes a secure and efficient platform. The inclusion of a user-friendly login and registration page facilitates secure access for individuals submitting objections to the police headquarters. The decentralized and immutable nature of the blockchain, coupled with the robust cryptographic mechanisms of the SHA-256 algorithm, ensures the authenticity and integrity of objection records. Moreover, the system incorporates specialized modules for the police headquarters and the admin, optimizing the handling and processing of objections. The utilization of blockchain technology not only guarantees transparency and accountability but also creates a tamper-proof and verifiable record of each objection submission. This not only fosters trust between the public and law enforcement but also streamlines the objection-handling process, marking a significant advancement in addressing public objections in criminal cases.

REFERENCES

[1]AN IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT G.Vasavi[1], Dr. G Kalpana [2] M.Tech[1], Professor of CSE [2] Department of Computer Science and Engineering, 8 August 2023

[2]BLOCKCHAIN-BASED SYSTEM FOR EFFECTIVE POLICE COMPLAINT MANAGEMENT Lynsha Helena Pratheeba HP, Associate professor, Bharath D R, Cibiya N E, Dheekshitha S, Divya M N, Department of Computer Science and Engineering, June 2023

[3]Blockchain-driven Evidence Management System by Shyam Mehta; K. Shantha Kumari; Paras Jain; Harshal Raikwar; Shubham Gore, 01 June 2023

[4]FIGAT: Accurately Classify Individual Crime Risks With Multi-Information BY Fusion Wenbo Xu, Peiyi Han, Shaoming Duan, and Chuanyi Liu,2023

[5]FIR SYSTEM USING BLOCKCHAIN TECHNOLOGY Bharath Kumar V, Dr. Mir Aadil, March 2023

[6]Impact of Crime Reporting System to Enhance Effectiveness of Police Service, KN Jayasinghe #1, MPL Perera#2 May 2021

[7]The Application of Blockchain of Custody in Criminal Investigation Process, Fu-Ching Tsai*, Department of Criminal Investigation, Central Police University, Taoyuan City 33304, Taiwan Volume 192, 2021

[8]Police Complaint Management System Using Blockchain Technology, Ishwarla Hingorani, Rushabh, Khara, Deepika, Pomendkar, Nataasharaul, 2020

[9]Sunil Yadav, Meet Timbadia, Ajit Yadav, Rohit Vishwakarma, and Nikhilesh Yadav, "Crime pattern detection, analysis and prediction, International Conference on Electronics, Communication and Aerospace Technology(ICECA), 2017

[10]A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT: Challenges and opportunities," Future Gener. Comput. Syst., vol. 88, pp. 173–190, 2018.

[11]M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," Comput. Secur., vol. 78, pp. 126–142, 2018.

[12]S. Chhabra, G. Gupta, M. Gupta, and G. Gupta, "Detecting fraudulent bank checks," in Proc. IFIP Int. Conf. Digit. Forensics, 2017, pp. 245–266.

[13]K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things, IEEE Access, vol. 4, pp. 2292–2303, 2016.

[14]Ubon Thansatapornwatana, "A Survey of Data Mining Techniques for Analyzing Crime Patterns", Second Asian Conference on Defense Technology ACDT, IEEE, Jan 2016, pp. 123–128

[15] H. Adel, M. Salheen, and R. Mahmoud, "Crime in relation to urban design. Case study: the greater Cairo region," Ain Shams Eng. J., vol. 7, no. 3, pp. 925-938, 2016.