Crime Alert: An Anonymous Crime Reporting System

Submitted for partial fulfillment of the requirements

for the award of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE ENGINEERING - ARTIFICIAL INTELLIGENCE & MACHINE LEARNING

by

Nandam Nagasivani	-	**20BQ1A4239**
Avula Srija Reddy	-	**20BQ1A4204**
Madduru Naga Sundeep	-	**20BQ1A4232**
Goddeti Vishnu Chaitanya	-	**21BQ5A4202**

Under the guidance of

K. Gnanendra, M. Tech

Assistant Professor

VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING - ARTIFICIAL INTELLIGENCE & MACHINE LEARNING

VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY

Permanently Affiliated to JNTU Kakinada, Approved by AICTE

Accredited by NAAC with 'A' Grade, ISO 9001:2008 Certified

NAMBUR (V), PEDAKAKANI (M), GUNTUR – 522 508

Tel no: 0863-2118036, url: www.vvitguntur.com

April 2024

VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY
Permanently Affiliated to JNTUK, Kakinada, Approved by AICTE
Accredited by NAAC with 'A' Grade, ISO 9001:20008 Certified
Nambur, Pedakakani (M), Guntur (Gt) -522508

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING - ARTIFICIAL INTELLIGENCE& MACHINE LEARNING

CERTIFICATE

This is to certify that this **Project Report** is the bonafide work of **Ms. Nagasivani Nandam, Ms. Srija Reddy Avula, Mr. Naga Sundeep Madduru, Mr. Vishnu Chaitanya Goddeti** bearing Reg. No. **20BQ1A4239, 20BQ1A4204, 20BQ1A4232, 21BQ5A4202** respectively who had carried out the project entitled **"Crime Alert: An Anonymous Crime Reporting System"** under our supervision.

Project Guide	**Head of the Department**
(Mr. K. Gnanendra, Assistant Professor)	(Dr. K. Suresh Babu, Professor)

Submitted for Viva voce Examination held on _____

Internal Examiner	**External Examiner**

DECLARATION

We, Ms. Nagasivani Nandam, Ms. Srija Reddy Avula, Mr. Naga Sundeep Madduru, Mr. Vishnu Chaitanya Goddeti, hereby declare that the Project Report entitled **"Crime Alert: An Anonymous Crime Reporting System"** done by us under the guidance of Mr. K. Gnanendra, Assistant Professor, Computer Science Engineering - Artificial Intelligence & Machine Learning at Vasireddy Venkatadri Institute of Technology is submitted for partial fulfillment of the requirements for the award of Bachelor of Technology in Computer Science Engineering - Artificial Intelligence and Machine Learning. The results embodied in this report have not been submitted to any other University for the award of any degree.

DATE :

PLACE :

SIGNATURE OF THE CANDIDATE (S)

Nandam Nagasivani

Avula Srija Reddy

Madduru Naga Sundeep

Goddeti Vishnu Chaitanya

ACKNOWLEDGEMENT

We take this opportunity to express my deepest gratitude and appreciation to all those people who made this project work easier with words of encouragement, motivation, discipline, and faith by offering different places to look to expand my ideas and helped me towards the successful completion of this project work.

First and foremost, we express my deep gratitude to **Mr. Vasireddy Vidya Sagar**, Chairman, Vasireddy Venkatadri Institute of Technology for providing necessary facilities throughout the B.Tech programme.

We express my sincere thanks to **Dr. Y. Mallikarjuna Reddy**, Principal, Vasireddy Venkatadri Institute of Technology for his constant support and cooperation throughout the B.Tech programme.

We express my sincere gratitude to **Dr. K. Suresh Babu**, Professor & HOD, Computer Science Engineering-Artificial Intelligence & Machine Learning, Vasireddy Venkatadri Institute of Technology for his constant encouragement, motivation and faith by offering different places to look to expand my ideas.

We would like to express my sincere gratefulness to our Guide **Mr. K. Gnanendra**, Assistant Professor, Computer Science Engineering-Artificial Intelligence & Machine Learning for his insightful advice, motivating suggestions, invaluable guidance, help and support in successful completion of this project.

We would like to express our sincere heartfelt thanks to our Project Coordinator **Mr. N. Balayesu**, Assistant Professor, Computer Science Engineering-Artificial Intelligence & Machine Learning, for his valuable advices, motivating suggestions, moral support, help and coordination among us in successful completion of this project.

We would like to take this opportunity to express my thanks to the **Teaching and Non-Teaching** Staff in the Department of Computer Science Engineering-Artificial Intelligence & Machine Learning, VVIT for their invaluable help and support.

Name (s) of Students:

Nandam Nagasivani

Avula Srija Reddy

Madduru Naga Sundeep

Goddeti Vishnu Chaitanya

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The Crime Alert: An Anonymous Crime Reporting System represents a paradigm shift in the realm of crime reporting platforms, offering a comprehensive solution for secure and confidential reporting of criminal activities. Through the adept utilization of cutting-edge technologies, including Convolutional Neural Networks (CNN) for robust data analysis and Blockchain Ethereum for immutable and transparent record-keeping, the system ensures unparalleled levels of reliability and integrity. By guaranteeing anonymity for whistleblowers and witnesses, the platform empowers individuals to report crimes without fear of reprisal, thereby fostering a culture of accountability and community safety. Leveraging CNN algorithms, the system efficiently processes and analyzes reported data, facilitating the rapid categorization and identification of patterns within reported incidents. The integration of Blockchain Ethereum further enhances data integrity and transparency by establishing a tamper-proof ledger of reported crimes, thereby bolstering trust in the system's efficacy and reliability. Each report is meticulously cryptographically secured, preventing unauthorized access or alteration, and reinforcing the system's commitment to preserving user privacy and data security. In summary, the Crime Alert: An Anonymous Crime Reporting System stands as a beacon of trust and innovation, heralding a new era of transparency and accountability in combating criminal activities.

Keywords: Anonymous Crime Reporting, Convolutional Neural Networks, CNN, Blockchain Ethereum, Secure Reporting, Data Analysis, Anonymity, Transparency, Immutable Records, Whistleblower Protection.

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND AND CONTEXT:

In our world today, crime is a serious concern that affects the safety and well-being of communities. However, many people are afraid to report crimes because they worry about their safety or privacy being compromised. Traditional ways of reporting crimes often do not offer enough protection for those who want to help.

That's where the Crime Alert: An Anonymous Crime Reporting System comes in. It's a new and smart way for people to report crimes without revealing who they are. This system uses special technology like Convolutional Neural Networks (CNN) and Blockchain Ethereum to keep everything safe and private. With Crime Alert, people can feel safe reporting crimes without worrying about what might happen to them.

The main idea behind Crime Alert is to make reporting crimes easier and safer for everyone involved. By using CNN algorithms, the system can quickly analyze the information people provide about crimes. This helps law enforcement understand patterns and trends in criminal activity, making it easier to catch criminals and keep communities safe.

Another important feature of Crime Alert is its use of Blockchain Ethereum. This technology ensures that all the information reported about crimes is stored securely and cannot be changed by anyone. It's like having a digital lockbox where important information is kept safe from prying eyes.

Our aim with Crime Alert is to aid law enforcement in creating a safer country where crime information is reported without hesitation. Reports by the National Crime Records Bureau reveal that 750,000 complaints are annually registered under the Indian Penal Code, often due to insufficient evidence. Studies indicate that 60% of crimes remain unreported. Collaboration between law enforcement and the public is crucial to combat crime and ensure community safety. The police require public assistance to prevent crime, combat criminality, and foster a secure society.

Overall, the Crime Alert: An Anonymous Crime Reporting System aims to create a safer and more trustworthy environment for reporting crimes. By protecting the anonymity of those who report crimes and using advanced technology to analyze and store information securely, Crime Alert helps communities work together to combat crime and keep everyone safe.

1.2 MOTIVATION:

The motivation behind the Crime Alert: An Anonymous Crime Reporting System stems from the urgent need to overcome barriers in reporting criminal activities. By integrating advanced technologies like Convolutional Neural Networks (CNN) for data analysis and Blockchain Ethereum for immutable record-keeping, Crime Alert: An Anonymous Crime Reporting System aims to provide a secure, confidential, and transparent platform. Its primary motivation lies in ensuring whistleblower protection, fostering trust through anonymity, and enabling efficient categorization of reported incidents. This system addresses the critical gaps in traditional reporting systems by offering a secure and trustworthy channel for reporting crimes without fear of reprisal, ultimately enhancing community safety and law enforcement effectiveness.

1.3 PROBLEM STATEMENT:

Traditional crime reporting systems often lack anonymity and security, deterring individuals from reporting criminal activities due to fear of retaliation or lack of trust in the confidentiality of the process. This leads to underreporting, hindering law enforcement's ability to address and prevent crimes effectively. Furthermore, centralized databases are susceptible to tampering, raising concerns about data integrity and transparency.

1.4 OBJECTIVE OF THE PROJECT:

1. Establish a secure and confidential platform: Develop a user-friendly interface that allows individuals to report criminal activities anonymously, ensuring their safety from potential reprisals.

2. Implement CNN for data analysis: Utilize advanced algorithms to process and analyze reported data, enabling efficient categorization and identification of patterns within incidents.

3. Integrate Blockchain Ethereum for transparency and immutability: Create a tamper-proof ledger of reported crimes, ensuring data integrity and transparency while preventing unauthorized access or modifications.

4. Ensure whistleblower protection: Safeguard the anonymity of whistleblowers and witnesses, encouraging them to report crimes without fear of exposure or retaliation.

5. Foster trust in the reporting system: Build a robust and reliable system that instills confidence in users, encouraging them to actively participate in reporting criminal activities without hesitation or distrust.

1.5 SCOPE:

The scope of the Crime Alert: An Anonymous Crime Reporting System encompasses the creation of a secure, confidential, and technologically advanced platform for reporting criminal activities. It involves the implementation of Convolutional Neural Networks (CNN) for robust data analysis and the integration of Blockchain Ethereum for immutable and transparent record-keeping. The system aims to ensure anonymity for whistleblowers and witnesses, fostering an environment where individuals can report crimes without fear of retaliation. The scope also involves the development of algorithms that efficiently process and categorize reported data to identify patterns within incidents. It extends to the establishment of a tamper-proof ledger using Blockchain Ethereum, ensuring data integrity and preventing unauthorized access or alterations. The primary focus is to create a trustworthy and secure environment that encourages reporting while safeguarding the anonymity of those involved.

1.6 PROJECT INTRODUCTION:

In an era marked by technological advancements, the need for a secure, confidential, and reliable system for reporting criminal activities has never been more pronounced. The Crime Alert: An Anonymous Crime Reporting System stands at the forefront of innovation, offering a pioneering solution to address this pressing societal need. Crime Alert: An Anonymous Crime Reporting System represents a paradigm shift in the way criminal incidents are reported and managed. It leverages cutting-edge technologies, notably Convolutional Neural Networks (CNN) for meticulous data analysis and Blockchain Ethereum for unassailable record-keeping, to create an ecosystem that ensures anonymity, integrity, and transparency in crime reporting. The core ethos of Crime Alert: An Anonymous Crime Reporting System revolves around providing a safe avenue for whistleblowers and witnesses to report criminal acts without the fear of retaliation or exposure. By enabling individuals to share crucial information anonymously, the system empowers them to contribute to the safety and security of their communities without compromising their safety.

The utilization of CNN algorithms within the system allows for the intricate processing and examination of reported data. This technological backbone enables the efficient categorization of incidents and the identification of recurring patterns, facilitating a deeper understanding of the dynamics of reported crimes. Moreover, the integration of Blockchain Ethereum technology plays a pivotal role in ensuring the immutability and transparency of the reported data. By harnessing the power of this decentralized ledger, Crime Alert: An Anonymous Crime Reporting System establishes an unalterable record of reported crimes, safeguarding against unauthorized access or tampering. This robust security measure fosters trust among users, stakeholders, and authorities in the veracity of the reported information. In essence, Crime Alert: An Anonymous Crime Reporting System heralds a new era in crime reporting, where cutting-edge technologies converge to uphold anonymity, data integrity, and transparency. It not only revolutionizes the process of reporting criminal activities but also serves as a beacon of trust and reliability in the pursuit of a safer and more just society.

1.7 SIGNIFICANCE OF THE STUDY:

The Crime Alert: An Anonymous Crime Reporting System is really important because it helps people report crimes in a safe and confidential way. This is a big deal because many traditional ways of reporting crimes don't keep people's identity secret, which can make them scared to report. By using fancy technology like Convolutional Neural Networks (CNN) and Blockchain Ethereum, this system keeps people anonymous and makes sure the information they provide is safe from being changed or seen by the wrong people. It's like having a secret box where you can share important information about crimes without anyone knowing who you are. This helps make communities safer and helps police do their job better.

1.8 OVERVIEW OF THE PROJECT:

The Crime Alert: An Anonymous Crime Reporting System is a smart way to report crimes without worrying about your identity being revealed. It uses special technology like Convolutional Neural Networks (CNN) and Blockchain Ethereum to keep everything safe and private. With this system, people can report crimes without being afraid of what might happen to them. It's like having a secret helper who keeps your information safe while still helping to catch bad guys. This project is a big step towards making reporting crimes easier and safer for everyone involved.

CHAPTER 2

LITERATURE SURVEY

2.1 RELATED WORK:

[1] B. Holtmann, and Domingo-Swarts, "Current trends and responses to crime in South Africa. Crime," Violence and Injury Prevention in South Africa, 2008, pp 105 - 129.

It reveals a complex landscape marked by high levels of crime, necessitating a multifaceted approach to violence and injury prevention. The research underscores the urgent need for effective strategies, highlighting the importance of community engagement and law enforcement collaboration. The study emphasizes the role of socio-economic factors and their impact on crime rates, advocating for targeted interventions to address underlying issues. Overall, the outcomes underscore the significance of comprehensive, evidence-based initiatives to combat crime and enhance safety in the South African context.

[2] Diva Lal, Adiba Abidin, Naveen Garg, and Vikas Deep. "Advanced immediate crime reporting to police in India." Procedia Computer Science, 85:543–549, 2016.

The implementation of advanced systems streamlines the reporting process, leading to quicker response times from law enforcement. Additionally, the study underscores the potential for increased public participation in crime reporting, contributing to a more responsive and proactive policing environment. The findings emphasize the positive impact of leveraging technology to augment crime reporting mechanisms, ultimately fostering a safer and more secure society in India.

[3] Tzay-Farn Shih, Chin-Ling Chen, Bo-Yan Syu, andYong-Yuan Deng. A cloud-based crime reporting system with identity protection. Symmetry, 11(2):255, 2019.

The implementation demonstrated enhanced security through identity protection measures, ensuring the confidentiality of reporters. Utilizing cloud technology improved accessibility and scalability, allowing users to submit reports seamlessly. The system's design, leveraging symmetry principles, contributed to a harmonized and efficient reporting process. The recorded outcomes showcased an advancement in user trust, encouraging individuals to engage in crime reporting. Overall, the study demonstrated the viability of a cloud-based approach with identity protection, offering a secure and user-friendly platform for reporting criminal incidents.

[4] Kovács, L., Szlávik, Z., Benedek, C., Havasi, L., Petrás, I., Losteiner, D., Utasi, Á., Liscár, A., Czúni, L. and Szirányi, T., "Video Surveillance Framework for Crime Prevention and Event Indexing," in ICT4Justice, January 2008.

The system employs advanced algorithms for event indexing, aiding in efficient crime detection and analysis. Through intelligent video processing, it enables automated monitoring and

identification of potential threats. The proposed framework not only contributes to crime prevention but also facilitates the systematic categorization and retrieval of relevant events. This research offers a valuable ICT tool for law enforcement, providing a proactive approach to enhance public safety through effective video surveillance and event indexing.

2.2 CURRENT TRENDS AND TECHNOLOGIES IN CRIME REPORTING SYSTEMS:

In recent years, there has been a significant evolution in crime reporting systems, driven by advancements in technology and changing societal needs. One notable trend is the increasing adoption of digital platforms and mobile applications for reporting crimes. These platforms offer convenient and accessible channels for individuals to report incidents, often enabling real-time communication with law enforcement agencies.

Moreover, there is a growing emphasis on enhancing the anonymity and confidentiality of crime reporting processes. Anonymous reporting systems leverage encryption techniques and secure communication protocols to protect the identity of whistleblowers and witnesses, thereby encouraging more people to come forward with valuable information.

Another emerging trend is the integration of artificial intelligence (AI) and machine learning algorithms in crime reporting systems. These technologies enable automated analysis of reported incidents, allowing law enforcement agencies to identify patterns, detect anomalies, and prioritize responses more effectively. Additionally, AI-powered chatbots and virtual assistants are being employed to provide immediate assistance to individuals reporting crimes, enhancing user experience and response times.
Blockchain technology has also gained traction in crime reporting systems, offering tamper-resistant and transparent record-keeping capabilities. By leveraging blockchain-based platforms, authorities can ensure the integrity and immutability of reported data, reducing the risk of data manipulation or tampering.

Furthermore, there is a growing recognition of the importance of community engagement and collaboration in crime prevention and reporting. Social media platforms and community-oriented applications are being utilized to facilitate information sharing, community policing initiatives, and empowering citizens to play an active role in maintaining public safety.

2.3 COMPARATIVE ANALYSIS OF EXISTING SOLUTIONS:

In comparing traditional crime reporting methods, internet-based systems, and camera surveillance with the new Crime Alert: An Anonymous Crime Reporting System, several distinctions emerge. Traditional approaches, like reporting to authorities directly, often lack mechanisms to ensure reporter anonymity, potentially dissuading individuals from coming forward due to fears of reprisal. In contrast, internet-based platforms offer improved anonymity through encryption and secure channels, making it safer for whistleblowers to report crimes without fear of exposure.

However, camera surveillance systems, while effective in providing visual evidence, may not prioritize protecting reporters' identities, focusing primarily on capturing events rather than ensuring anonymity.

When it comes to data analysis capabilities, traditional methods and camera surveillance systems may struggle to efficiently process and analyze reported data to discern patterns or trends in criminal activities. Internet-based systems typically fare better, utilizing basic analytics tools to understand collected data. Nevertheless, the Crime Alert system excels by employing advanced technologies such as Convolutional Neural Networks (CNN) for robust data analysis. This enables quick identification of patterns within reported incidents, enhancing the system's capacity to categorize and analyse crime reports effectively, providing valuable insights for law enforcement and community safety.

In terms of transparency and reliability, traditional methods and camera surveillance systems may face challenges in ensuring data integrity and trustworthiness due to centralized storage and potential tampering. Internet-based systems mitigate these concerns by employing decentralized storage and immutable records, enhancing trust in reported information. However, the Crime Alert system surpasses existing solutions by leveraging Blockchain Ethereum technology for transparent and tamper-proof record-keeping. This ensures data integrity and reliability, instilling confidence among users, stakeholders, and law enforcement agencies in the accuracy and authenticity of reported crime information

CHAPTER 3

ANALYSIS & DESIGN

3.1 SYSTEM ANALYSIS

3.1.1 OVERVIEW OF EXISTING CRIME REPORTING SYSTEMS

Existing crime reporting systems often lack robust mechanisms for ensuring the anonymity and security of individuals reporting criminal activities. Traditional systems often rely on manual reporting methods, which may deter whistleblowers and witnesses due to concerns about potential reprisals or breaches of confidentiality. These systems might also lack advanced data analysis tools, making it challenging to efficiently categorize and identify patterns within reported incidents. Furthermore, the absence of secure record-keeping methods could compromise the integrity and transparency of reported data, leading to potential tampering or unauthorized access.

3.1.2 IDENTIFICATION OF LIMITATIONS AND CHALLENGES:

1. Lack of Anonymity: Many existing systems fail to provide adequate anonymity to whistleblowers and witnesses, discouraging individuals from reporting crimes due to fear of retaliation or exposure.

2. Insufficient Security Measures: Traditional reporting systems often lack robust security measures, making them vulnerable to data breaches, hacking attempts, or unauthorized access, compromising the confidentiality of reported information.

3. Limited Data Analysis Capabilities: These systems may lack advanced technologies like machine learning or neural networks, making it challenging to analyze reported data efficiently and identify crucial patterns or trends in criminal activities.

4. Vulnerability to Tampering: Without proper record-keeping mechanisms, existing systems are susceptible to data tampering or alterations, undermining the integrity and reliability of reported crime information.

5. Lack of Transparency: The absence of transparent and immutable record-keeping methods can result in a lack of trust in the reported data's accuracy and authenticity, leading to scepticism among users and authorities regarding the reliability of the system.

3.1.3 PROPOSED SYSTEM

The Crime Alert: An Anonymous Crime Reporting System is a cutting-edge solution poised to revolutionize the landscape of crime reporting. This innovative platform is designed with a primary focus on security and confidentiality, enabling individuals to report criminal activities without the fear of exposure or retaliation. Utilizing advanced technologies like Convolutional Neural Networks (CNN) for intricate data analysis and Blockchain Ethereum for immutable record-keeping, the Crime Alert: An Anonymous Crime Reporting System ensures anonymity for whistleblowers and witnesses. Through the integration of CNN algorithms, the system efficiently processes and categorizes reported data, allowing for the identification of patterns within incidents. Meanwhile, the incorporation of Blockchain Ethereum guarantees data integrity and transparency, establishing an unalterable ledger of reported crimes, fostering trust and reliability in the system's operations.

3.1.4 ADVANTAGES

1. Anonymity Protection: The system prioritizes whistleblower safety by providing a secure environment for reporting, safeguarding identities and enabling individuals to disclose criminal activities without fear of retaliation.

2. Efficient Data Analysis: Leveraging CNN algorithms, the Crime Alert: An Anonymous Crime Reporting System can swiftly process and categorize vast amounts of reported data, facilitating quicker identification of patterns and trends within criminal incidents.

3. Immutable Record-Keeping: Utilizing Blockchain Ethereum technology ensures that reported crime data remains tamper-proof and transparent. This fosters trust among users and stakeholders regarding the integrity of the information stored.

4. Transparency and Trust: The system's use of Blockchain technology promotes transparency, creating a clear and verifiable trail of reported incidents. This transparency enhances trust among users, law enforcement agencies, and the community.

5. Robust Security Measures: With cryptographic security measures in place, unauthorized access or alterations to reported data are prevented, ensuring the system's resilience against potential cyber threats or tampering attempts, thereby maintaining the credibility

3.1.5 WORK FLOW OF PROPOSED SYSTEM

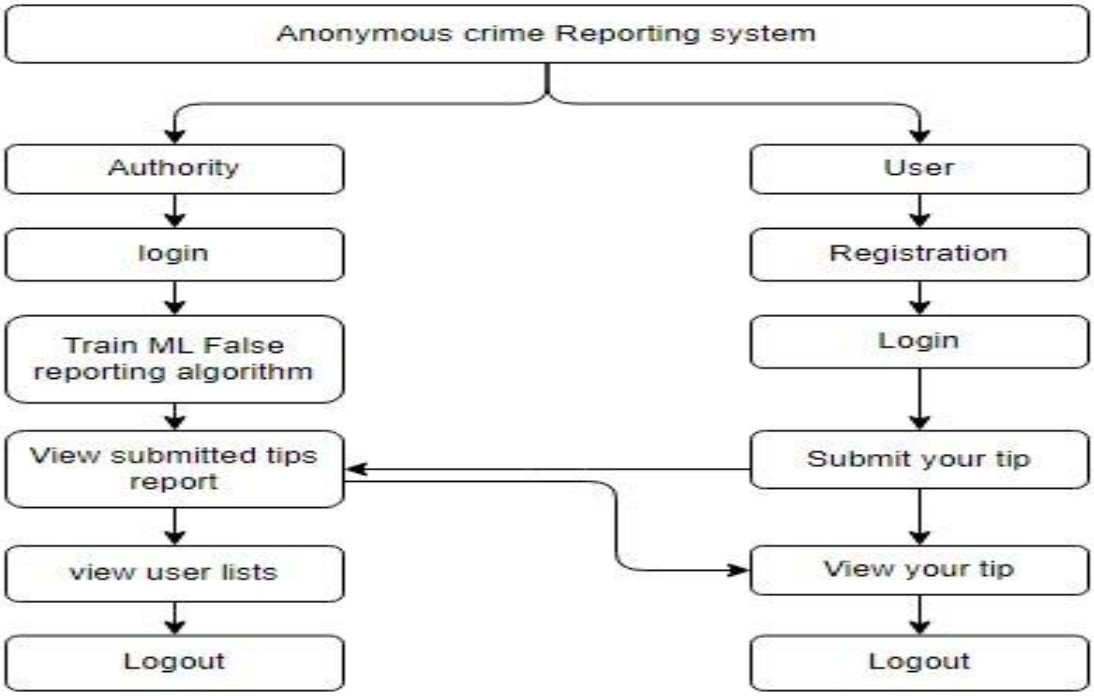


Fig:3.1 Work Flow of Proposed System

3.2 REQUIREMENT ANALYSIS

3.2.1 FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

Requirement's analysis is very critical process that enables the success of a system or software project to be assessed. Requirements are generally split into two types: Functional and non-functional requirements.

Functional Requirements: These are the requirements that the end user specifically demands as basic facilities that the system should offer. All these functionalities need to be necessarily incorporated into the system as a part of the contract. These are represented or stated in the form of input to be given to the system, the operation performed and the output expected.

They are basically the requirements stated by the user which one can see directly in the final product, unlike the non-functional requirements.

Examples of functional requirements:

1) Authentication of user whenever he/she logs into the system
2) System shutdown in case of a cyber-attack
3) A verification email is sent to user whenever he/she registers for the first time on some software system.

Non-functional requirements: These are basically the quality constraints that the system must satisfy according to the project contract. The priority or extent to which these factors are implemented varies from one project to other. They are also called non-behavioral requirements. They basically deal with issues like:

- Portability
- Security
- Maintainability
- Reliability
- Scalability
- Performance
- Reusability
- Flexibility

Examples of non-functional requirements:

1) Emails should be sent with a latency of no greater than 12 hours from such an activity.
2) The processing of each request should be done within 10 seconds
3) The site should load in 3 seconds whenever of simultaneous users are > 10000

3.2.2 HARDWARE REQUIREMENTS:

Processor	- I3/Intel Processor
Hard Disk	- 160GB
Key Board	- Standard Windows Keyboard
Mouse	- Two or Three Button Mouse
Monitor	- SVGA
RAM	- 8GB

3.2.3 SOFTWARE REQUIREMENTS:

Frontend	- HTML5/CSS, JavaScript, Bootstrap, Node-js
Programming languages	- Solidity Programming, Python
Backend & Database	- Django, SQLIte
Blockchain Ecosystem	- Ethereum
Frameworks	- TensorFlow, Truffle, Keras, Django
Library	- Scikit-learn, Pandas, NumPy, NLTK, Web3
Version control system	- Git, Github
Testing Framework	- Selenium
User Interface Design Tools	- Figma
Deploying Platform	- AWS/Azure

3.2.4 ARCHITECTURE:

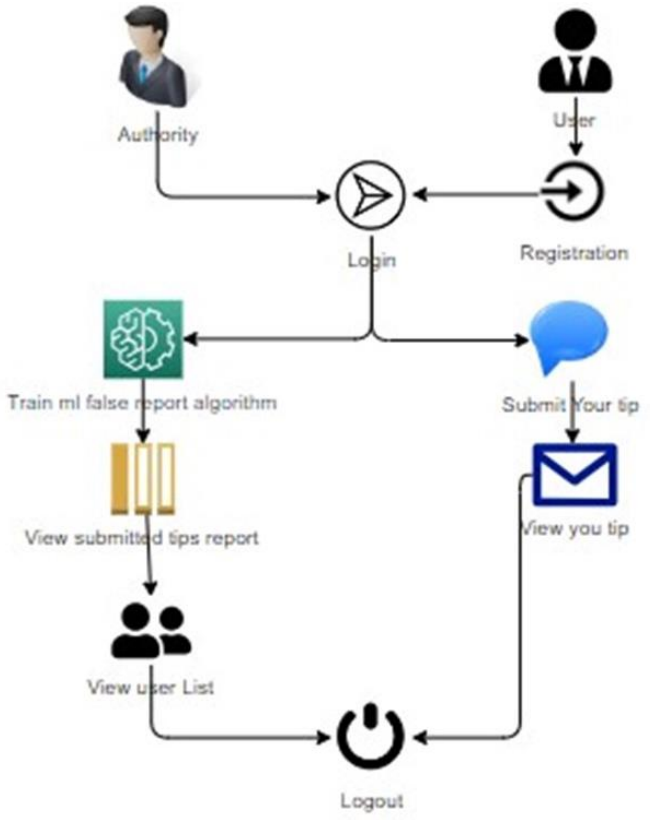


Fig:3.2 Proposed System Architecture

3.3 TECHNOLOGIES USED

Frontend Technologies:

HTML (Hypertext Markup Language): HTML is the standard markup language for creating web pages and applications. It provides the structure and layout for web content, using elements and tags to define different parts of a webpage such as headings, paragraphs, links, and images. In the Crime Alert system, HTML is utilized to create the user interface, defining the layout and structure of the reporting platform.

CSS (Cascading Style Sheets): CSS is a style sheet language used to enhance the presentation of HTML documents. It allows developers to customize the appearance of web pages by specifying styles such as colors, fonts, spacing, and layout. In the Crime Alert system, CSS is employed to apply styles to HTML elements, ensuring a visually appealing and user-friendly interface for reporting criminal activities.

Bootstrap: Bootstrap is a popular front-end framework that simplifies the process of designing responsive and mobile-first websites. It provides pre-designed components and CSS stylesheets that developers can use to create consistent and visually appealing interfaces across different devices and screen sizes. In the Crime Alert system, Bootstrap is utilized to enhance the responsiveness and accessibility of the reporting platform, ensuring optimal user experience on various devices.

JavaScript (JS): JavaScript is a versatile programming language commonly used for adding interactivity and dynamic behaviour to web pages. It enables developers to create interactive elements, handle user input, manipulate the DOM (Document Object Model), and communicate with backend servers asynchronously. In the Crime Alert system, JavaScript is employed to implement interactive features such as form validation, real-time updates, and user feedback, enhancing the functionality and usability of the reporting platform.

Node.js: Node.js is an open-source, cross-platform runtime environment for executing JavaScript code on the server side. It enables developers to build scalable and high-performance server-side applications using JavaScript, taking advantage of its non-blocking, event-driven architecture.

Backend Technologies:

Python: Python is a high-level, interpreted programming language known for its simplicity, readability, and versatility. It is widely used for backend web development due to its extensive libraries, frameworks, and support for various programming paradigms. In the context of this project, Python is used for implementing machine learning algorithms, handling data processing, and managing server-side logic.

SQLite: SQLite is a small and easy-to-use database system that doesn't need a separate server. It stores data directly in a single file on your device. You can use it to organize and manage information for your crime alert project, like details about incidents, suspects, and locations. It follows standard SQL commands, making it simple to learn and use. Despite being lightweight, it supports essential features like transactions and data integrity. SQLite is great for projects with limited resources or when you want a quick and straightforward way to store and retrieve data. Its simplicity and portability make it a popular choice for many applications

Django: Django is a high-level, open-source Python web framework that encourages rapid development and clean, pragmatic design. Built on the Model-View-Template (MVT) architectural pattern, it simplifies the process of creating complex web applications by providing a rich set of built-in components and tools. Django promotes best practices, including separation of concerns, reusability, and maintainability, and offers an extensive range of features, such as an Object-Relational Mapper (ORM) system, an admin interface, and authentication mechanisms. Its simplicity and scalability make it an ideal choice for both small projects and large-scale, enterprise-level web applications

Blockchain Ecosystem

Ethereum: Ethereum, as an open-source, blockchain-based, decentralized software platform, serves as the foundation for the Crime Alert: An Anonymous Crime Reporting System. It enables the creation and execution of Smart Contracts, which form the backbone of the secure tip reporting and verification process. Ethereum's blockchain technology ensures the immutability and transparency of the reported data, making it a reliable and trustworthy system for anonymous crime tip reporting.

Solidity: Solidity, a contract-oriented, high-level programming language, is used to write Smart Contracts for Ethereum in the Crime Alert system. It provides static typing, explicit modeling, and features such as inheritance, libraries, and complex user-defined types, which contribute to the creation of modular and reusable Smart Contracts. By employing Solidity in the project, the system can maintain secure and automated tip reporting and verification processes, ensuring the anonymity and security of tip submitters while maintaining the integrity and transparency of the reported data.

Frameworks:

TensorFlow: TensorFlow is an open-source machine learning and deep learning framework developed by Google. It provides a comprehensive ecosystem of tools, libraries, and community resources for training, deploying, and scaling machine learning models across various platforms and architectures.

Truffle: Truffle is a development framework for Ethereum Smart Contracts. It provides a suite of tools and features for compiling, deploying, and testing Solidity contracts, including a local development blockchain, automated contract deployment, and a scriptable configuration system**.**

Keras: Keras is a high-level neural networks API, written in Python and capable of running on top of TensorFlow, Theano, or Microsoft Cognitive Toolkit (CNTK). It provides a user-friendly interface for building and training deep learning models, with support for both convolutional and recurrent neural networks. Keras emphasizes simplicity, flexibility, and extensibility, making it suitable for beginners and experienced practitioners alike.

Libraries:

Scikit-learn: Scikit-learn is a Python library for machine learning, specifically designed for data mining and data analysis. It provides a wide range of algorithms, tools, and functionalities for classification, regression, clustering, and dimensionality reduction, accessible through a simple and consistent interface. It is built on top of NumPy, SciPy, and matplotlib, making it easy to integrate into existing Python workflows. scikit-learn plays a crucial role in the Crime Alert system by enabling the development of robust and accurate machine learning models for predicting and identifying crime patterns thereby enhancing public safety and security.

Pandas: Pandas is a powerful data manipulation and analysis library for Python, commonly used for handling structured data such as tables and time series. It provides data structures like Data Frame and Series, along with functions for data cleaning, transformation, aggregation, and visualization. In the Crime Alert system, Pandas is employed for processing and analysing reported crime data, enabling efficient categorization, pattern recognition, and trend identification.

NumPy: NumPy is a fundamental library for scientific computing in Python, providing support for multidimensional arrays, mathematical functions, and linear algebra operations. It offers efficient data storage and manipulation capabilities, along with tools for numerical analysis, statistical modeling, and machine learning. In the Crime Alert system, NumPy is used for numerical computations, statistical analysis, and machine learning algorithms applied to crime data processing and analysis.

NLTK: NLTK (Natural Language Toolkit) is a leading platform for building Python programs that work with human language data. It provides easy-to-use interfaces to over 50 corpora and lexical resources, along with a suite of text processing libraries for tokenization, parsing, and semantic reasoning.

Web3.py: Web3.py is a Python library for interacting with Ethereum, providing an easy-to-use interface for connecting to Ethereum nodes, executing transactions, and interacting with Smart Contracts. It serves as a bridge between Python applications and the Ethereum blockchain, enabling seamless integration and communication.Web3.py simplifies the process of building Ethereum-based applications by providing a high-level API for interacting with smart contracts and blockchain data.

IPFS (InterPlanetary File System): IPFS is a decentralized, content-addressable, and peer-to-peer file system protocol designed to store and share hypermedia in a distributed manner. It aims to provide a more efficient, secure, and resilient alternative to traditional HTTP-based web architectures by utilizing a unique combination of content-addressing, block exchange, and versioning. In the context of the Crime Alert: An Anonymous Crime Reporting System, IPFS can be employed to store and distribute large files, such as multimedia evidence, associated with crime reports securely and efficiently.

PyAES: PyAES is a Python library that provides an implementation of AES (Advanced Encryption Standard), a symmetric encryption algorithm widely recognized for its high level of security and

efficiency. In the context of the Crime Alert system, PyAES can be employed to encrypt and decrypt sensitive information, such as user data, ensuring the confidentiality and integrity of the information exchanged between the system and its users.

PBKDF2 (Password-Based Key Derivation Function 2): PBKDF2 (Password-Based Key Derivation Function 2) is a password-hashing method that uses an iterative process to generate a cryptographic key from a password or passphrase. The function aims to mitigate the risk of brute-force attacks by introducing computational complexity, making it harder and more time-consuming to crack the derived key.

These technologies collectively form the backbone of the Crime Alert system, enabling the development of a secure, efficient, and user-friendly platform for reporting criminal activities, analysing crime data, and ensuring transparency and accountability in the reporting process.

3.4 ALGORITHMS:

3.4.1 CONVOLUTIONAL NEURAL NETWORK (CNN):

Convolutional Neural Network (CNN) is a type of deep learning model commonly utilized for various tasks in computer vision, natural language processing, and sequential data analysis. CNN have been successfully applied to various natural language processing tasks, including text classification, sentiment analysis, and language translation. In text classification, for instance, CNN can effectively analyze textual data by learning meaningful patterns and relationships between words or phrases. By processing input text through multiple convolutional and pooling layers, CNN can capture important linguistic features and contextual information, enabling accurate classification of text into different categories or labels. The hierarchical nature of CNN architectures allows them to learn complex representations of text data, making them particularly adept at handling tasks that involve analyzing sequential information. With their versatility and capability to automatically learn from data, CNN continue to be at the forefront of research and development in the field of deep learning and artificial intelligence.

3.4.2 BLOCKCHAIN (ETHEREUM):

Blockchain is a decentralized and distributed ledger technology that enables the secure and transparent recording of transactions across a network of computers. Ethereum is a blockchain platform that extends the functionality of traditional blockchain by introducing smart contracts, which are self-executing contracts with predefined conditions written in code.

In Ethereum's blockchain, each block contains a list of transactions, and every block is linked to the previous one, forming a chronological chain of blocks. This linkage, along with cryptographic hashing and consensus mechanisms, ensures the immutability and security of the data recorded on the blockchain. Ethereum's smart contracts enable the execution of complex logic and the creation of decentralized applications (DApps) that operate autonomously and transparently without the need for intermediaries.

3.5 INTEGRATION POINTS AND USE CASES

3.5.1 UTILIZATION OF CNN FOR FALSE ALARM DETECTION

Utilizing Convolutional Neural Networks (CNNs) in the Crime Alert: An Anonymous Crime Reporting System focuses primarily on text-related tasks, particularly in detecting false alarms within reported incidents. Initially, the text descriptions undergo preprocessing to eliminate stop words, punctuation, and other irrelevant information, ensuring that only useful features are retained. Subsequently, these pre-processed descriptions are converted into numerical representations through word embedding, capturing the semantic meaning of words and their relationships within the text.

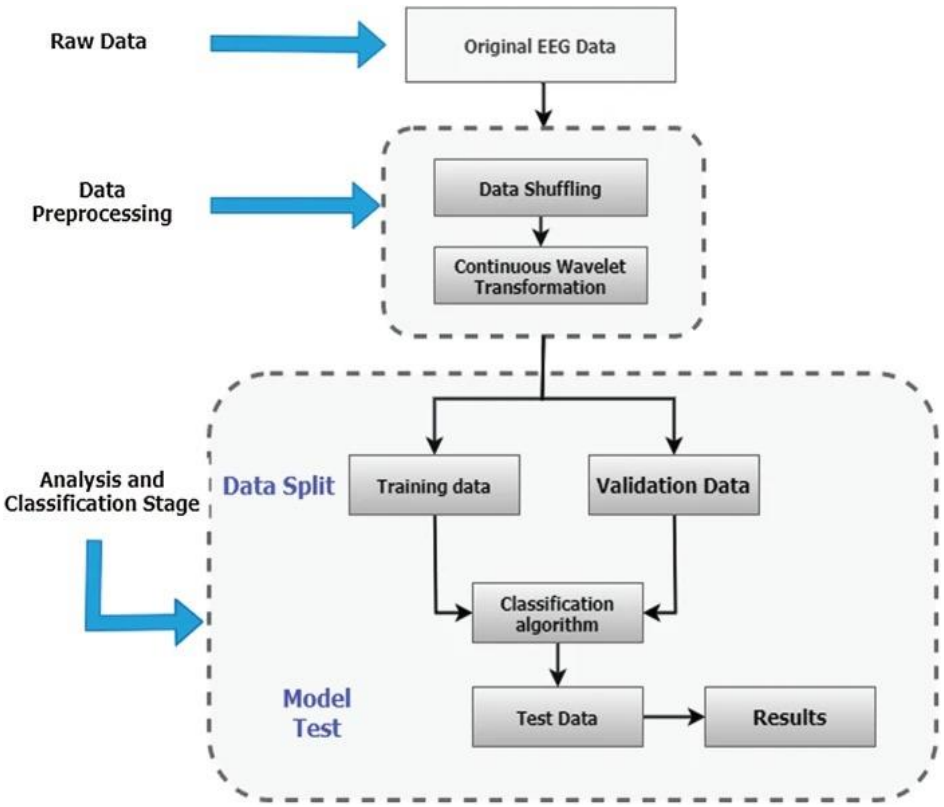


Fig:3.3 CNN algorithm for False Alarm Detection

Data Preprocessing:
The text descriptions in the dataset undergo preprocessing to remove stop words, punctuation, and other irrelevant information, ensuring that only useful features are retained. This initial preprocessing step enhances the quality and relevance of the text data for subsequent analysis.

Word Embedding:
Following preprocessing, the text descriptions are converted into numerical representations through word embedding. This process captures the semantic meaning of words and their relationships within the text, facilitating deeper analysis by the CNN model. By embedding the preprocessed text descriptions into numerical vectors, the CNN can effectively analyze and interpret the textual data.

Data Split:
The preprocessed and embedded text descriptions are then divided into training, validation, and test datasets. The training dataset is utilized to train the CNN model, where it learns to extract pertinent features from the text descriptions. This data splitting ensures that the model is trained on a diverse set of examples and prevents overfitting to the training data.

CNN Model:
A CNN model is trained on the embedded text descriptions to classify the reports as genuine or false. Through a series of convolutional and pooling layers, the CNN identifies intricate patterns and characteristics indicative of genuine criminal activities. The extracted features are then fed into fully connected layers for classification, enabling the CNN model to discern between genuine and false alarms based on the patterns learned during training. The model's performance is evaluated using a separate validation dataset, computing metrics such as accuracy, precision, recall, and F1 score to assess its effectiveness in accurately identifying false alarms. This meticulous process ensures the reliability and robustness of the CNN model in enhancing the accuracy of the Crime Alert system.

3.5.2 INCORPORATION OF BLOCKCHAIN FOR ANONYMOUS TIP SUBMISSION

The Crime Alert system integrates Blockchain Ethereum technology to facilitate secure and anonymous tip submission, ensuring the confidentiality and integrity of the reported information. Blockchain serves as the foundation for creating a tamper-proof and transparent ledger of reported crimes, safeguarding against unauthorized access or alterations while maintaining anonymity for whistleblowers.

Key Features:
Immutable Ledger: Each tip report is cryptographically hashed and added to the Ethereum blockchain, creating an immutable record that cannot be modified or tampered with. This ensures the integrity and transparency of the reported data.

Anonymity Protection: Blockchain technology allows users to submit tips anonymously without revealing their identities. User anonymity is preserved throughout the submission process, fostering a safe and confidential environment for reporting criminal activities.

Decentralized Architecture: The decentralized nature of Blockchain Ethereum eliminates the need for a central authority or intermediary, reducing the risk of data manipulation or corruption. This enhances trust in the reporting system among users and stakeholders.

Transparent Verification: Tip reports stored on the blockchain can be transparently verified by authorized parties, ensuring the authenticity and reliability of the information. This transparency promotes accountability and trust in the reported data.

Ethereum is used primarily for secure and transparent data storage through its blockchain technology.

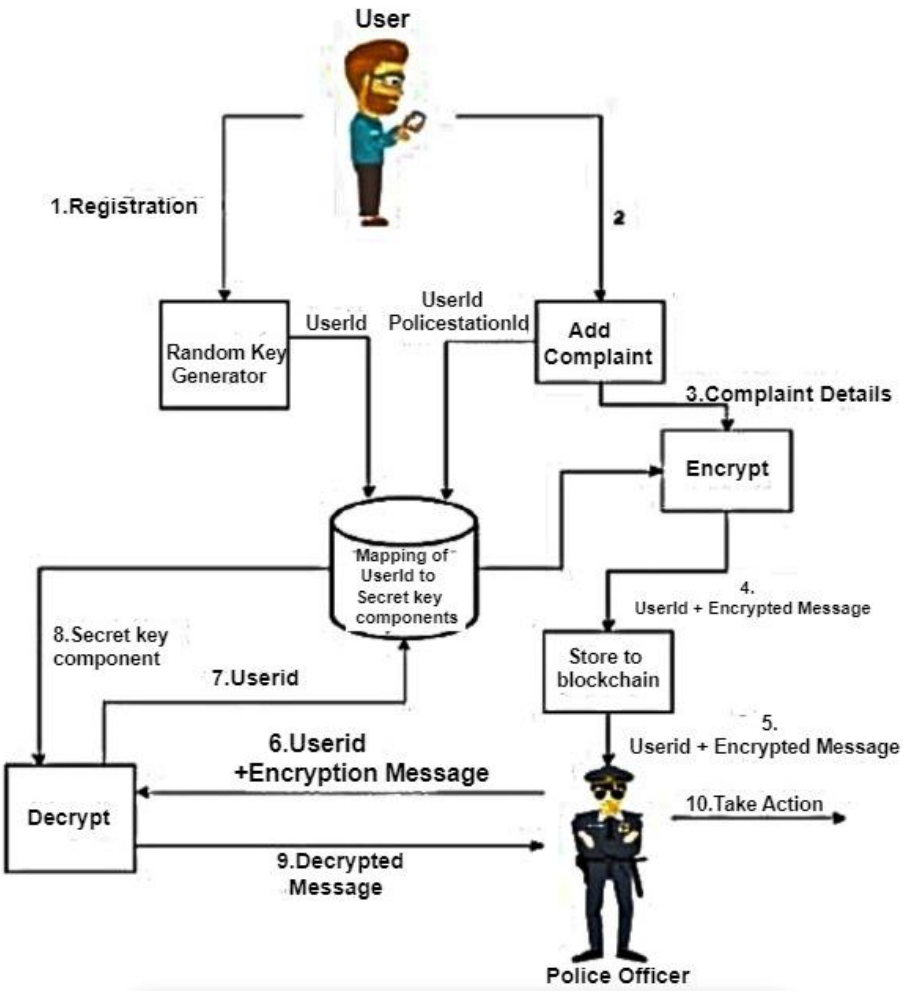


Fig:3.4 Blockchain Architecture

- **Registration:** Ethereum is not directly involved in the registration process of generating random keys and creating secret key components. This step is primarily focused on ensuring user anonymity.

- **User id Generation:** Similarly, Ethereum is not directly involved in generating User ids. This step mainly involves creating unique identifiers for users, which are mapped to their secret key components.

- **Encrypted Message Sending:** Ethereum is not directly involved in the encryption and sending of messages. Users encrypt messages using their secret key components, ensuring secure transmission to the system.

- **Decryption:** Ethereum does not participate in the decryption process. The system decrypts received messages using the appropriate secret key components, which were generated during registration.

- **Complaint Details Storage:** Here is where Ethereum comes into play. And stored on a blockchain, associated with the user's Userid, ensuring data integrity and transparency.

The Crime Alert: An Anonymous Crime Reporting System leverages Ethereum's blockchain technology to ensure secure and transparent crime reporting. Smart contracts on the Ethereum blockchain facilitate the creation of immutable and tamper-proof records for reported incidents. Each report is timestamped, encrypted, and linked to a unique identifier, enhancing anonymity while maintaining data integrity. Ethereum's decentralized nature eliminates the need for a central authority, reducing the risk of corruption.

Additionally, the system employs cryptographic techniques for secure user identification, providing a reliable and confidential channel for reporting crimes. This innovative blockchain solution fosters trust and accountability in crime reporting, paving the way for a safer and more secure community

3.6 SYSTEM DESIGN

INTRODUCTION OF INPUT DESIGN:

In an information system, input is the raw data that is processed to produce output. During the input design, the developers must consider the input devices such as PC, MICR, OMR, etc.

Therefore, the quality of system input determines the quality of system output. Well-designed input forms and screens have following properties −

- It should serve specific purpose effectively such as storing, recording, and retrieving the information.

- It ensures proper completion with accuracy.

- It should be easy to fill and straightforward.
- It should focus on user's attention, consistency, and simplicity.
- All these objectives are obtained using the knowledge of basic design principles regarding−
    - What are the inputs needed for the system?
    - How end users respond to different elements of forms and screens.

Objectives for Input Design:

The objectives of input design are −

- To design data entry and input procedures
- To reduce input volume
- To design source documents for data capture or devise other data capture methods
- To design input data records, data entry screens, user interface screens, etc.
- To use validation checks and develop effective input controls.

Output Design:

The design of output is the most important task of any system. During output design, developers identify the type of outputs needed, and consider the necessary output controls and prototype report layouts.

Objectives of Output Design:

The objectives of input design are:

- To develop output design that serves the intended purpose and eliminates the production of unwanted output.
- To develop the output design that meets the end user's requirements.
- To deliver the appropriate quantity of output.
- To form the output in appropriate format and direct it to the right person.
- To make the output available on time for making good decisions.

3.7 UML DIAGRAMS:

UML stands for Unified Modelling Language. UML is a standardized general-purpose modelling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object-oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modelling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modelling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modelling of large and complex systems.

The UML is a very important part of developing objects-oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS:

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modelling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modelling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

USE CASE DIAGRAM

- A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis.

- Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases.

- The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

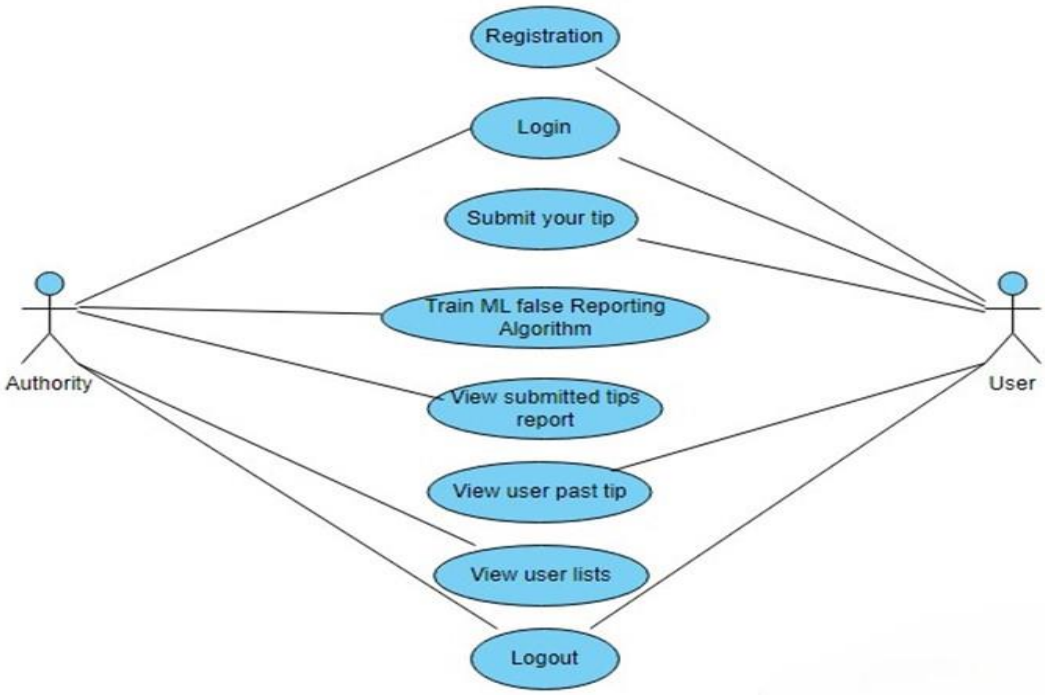


Fig:3.5 Use Case Diagram

CLASS DIAGRAM

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information

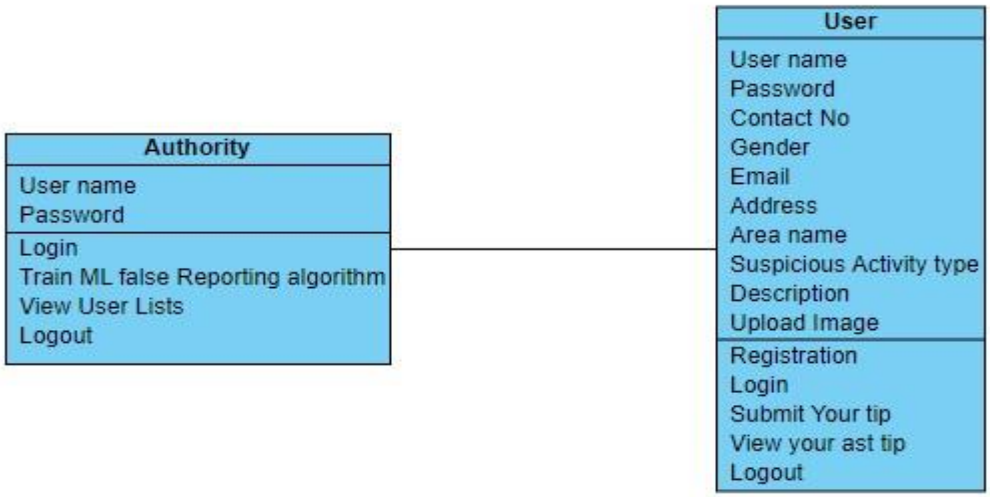


Fig:3.6 Class Diagram

SEQUENCE DIAGRAM

- A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order.
- It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams

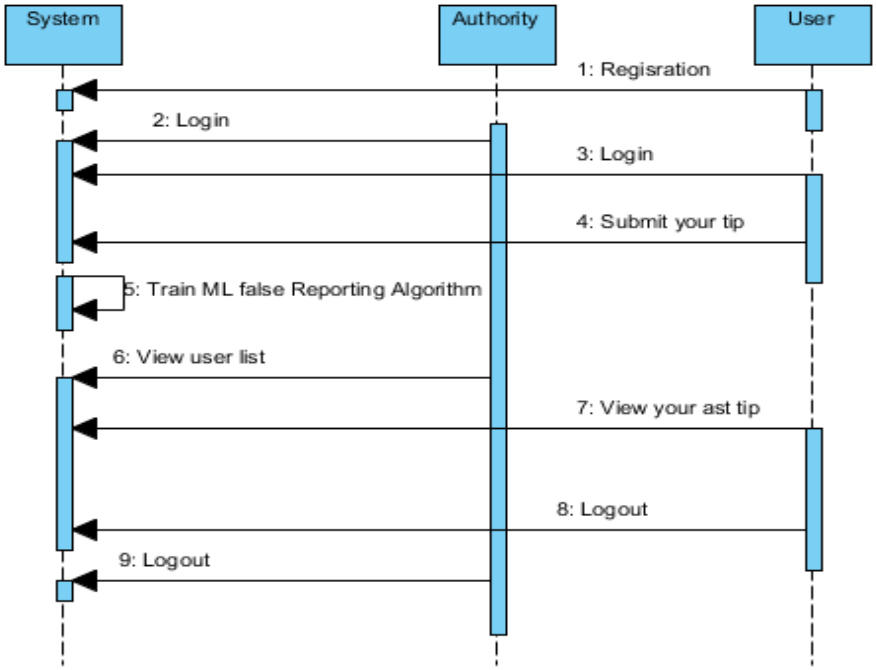


Fig:3.7 Sequence Diagram

COLLABORATION DIAGRAM:

In collaboration diagram the method call sequence is indicated by some numbering technique as shown below. The number indicates how the methods are called one after another. We have taken the same order management system to describe the collaboration diagram. The method calls are similar to that of a sequence diagram. But the difference is that the sequence diagram does not describe the object organization whereas the collaboration diagram shows the object organization.

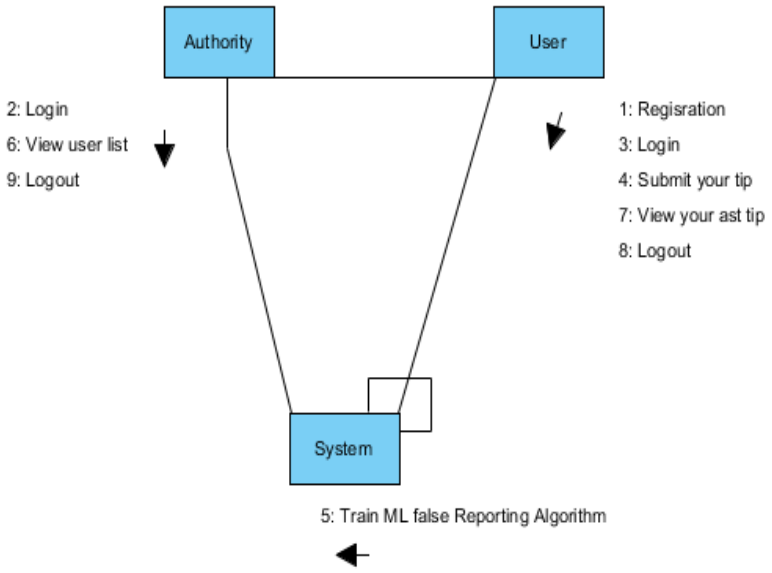


Fig:3.8 Collaboration Diagram

DEPLOYMENT DIAGRAM

Deployment diagram represents the deployment view of a system. It is related to the component diagram. Because the components are deployed using the deployment diagrams. A deployment diagram consists of nodes. Nodes are nothing but physical hardware's used to deploy the application.

Fig:3.9 Deployment Diagram

ACTIVITY DIAGRAM:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

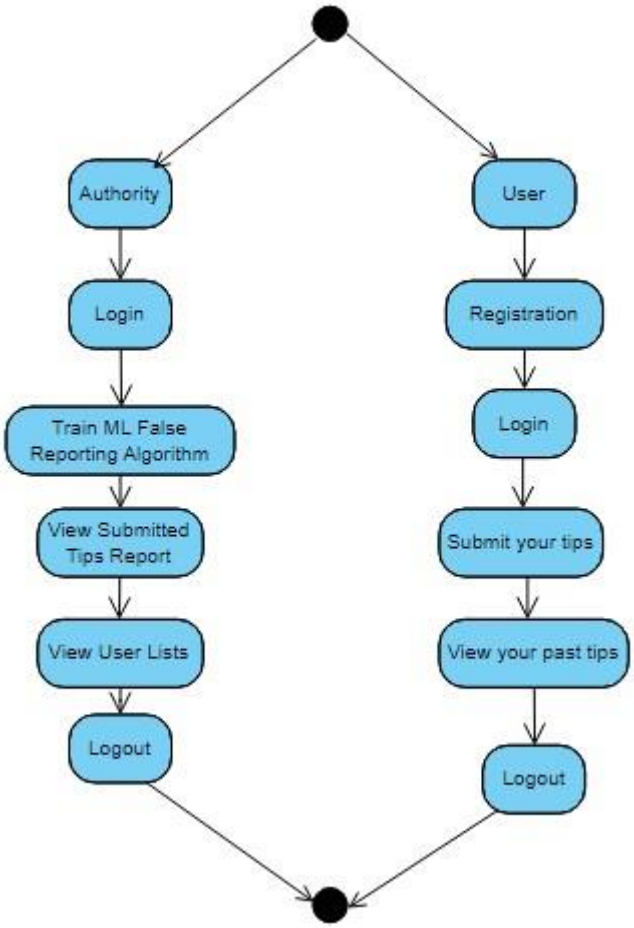


Fig:3.10Activity Diagram

COMPONENT DIAGRAM:

A component diagram, also known as a UML component diagram, describes the organization and wiring of the physical **c**omponents in a system. Component diagrams are often drawn to help model implementation details and double-check that every aspect of the system's required function is covered by planned development.

Fig:3.11 Component Diagram

ER DIAGRAM:

An Entity–relationship model (ER model) describes the structure of a database with the help of a diagram, which is known as Entity Relationship Diagram (ER Diagram). An ER model is a design or blueprint of a database that can later be implemented as a database. The main components of E-R model are: entity set and relationship set.

An ER diagram shows the relationship among entity sets. An entity set is a group of similar entities and these entities can have attributes. In terms of DBMS, an entity is a table or attribute of a table in database, so by showing relationship among tables and their attributes, ER diagram shows the complete logical structure of a database. Let's have a look at a simple ER diagram to understand this concept.

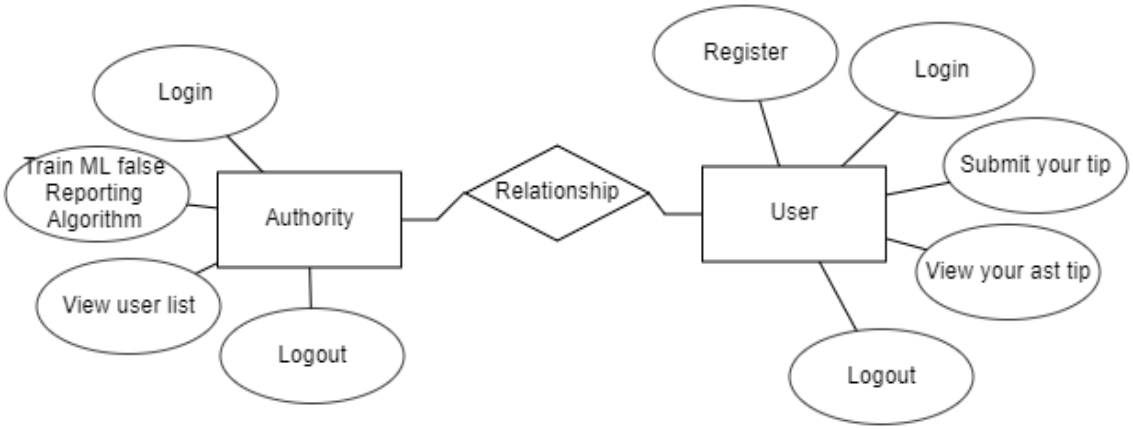


Fig:3.12 ER Diagram

DFD DIAGRAM:

A Data Flow Diagram (DFD) is a traditional way to visualize the information flows within a system. A neat and clear DFD can depict a good amount of the system requirements graphically. It can be manual, automated, or a combination of both. It shows how information enters and leaves the system, what changes the information and where information is stored. The purpose of a DFD is to show the scope and boundaries of a system as a whole. It may be used as a communications tool between a systems analyst and any person who plays a part in the system that acts as the starting point for redesigning a system.

DFD LEVEL-1 DIAGRAM

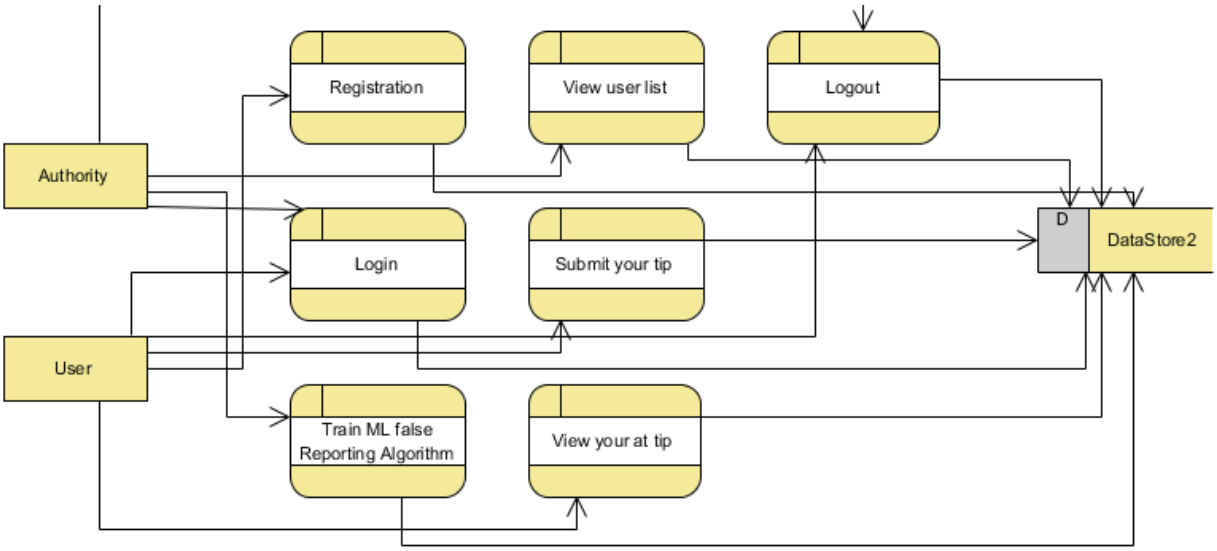


Fig:3.13 DFD Level-1 Diagram

DFD LEVEL-2 DIAGRAM

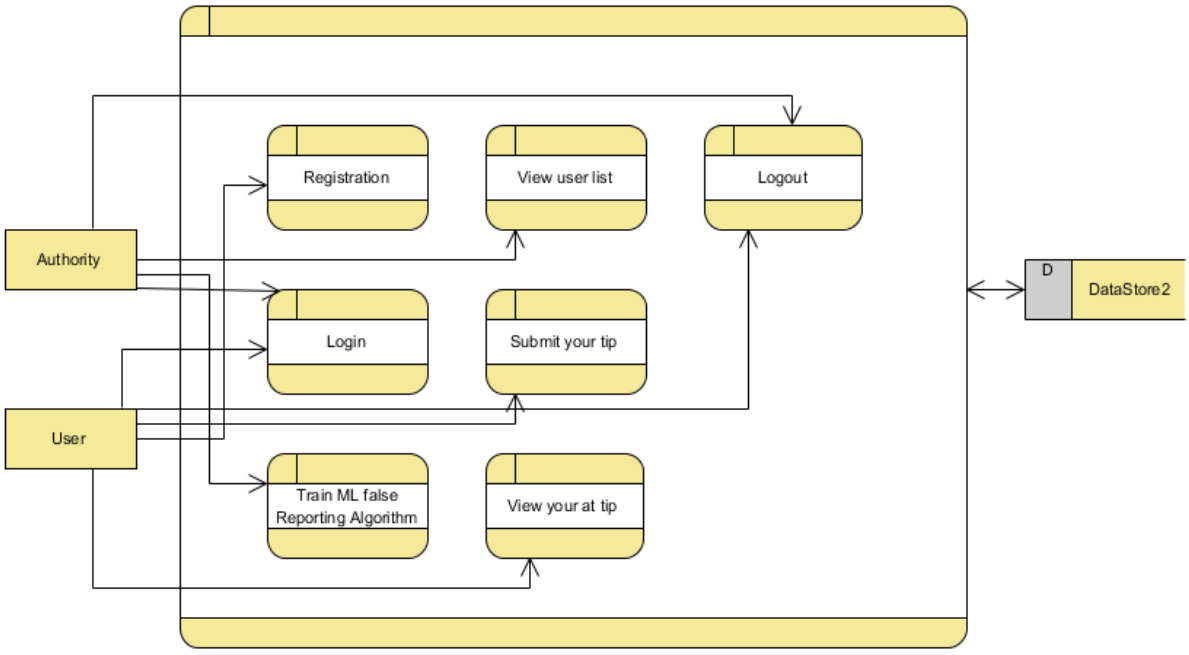


Fig:3.14 DFD Level-2 Diagram

CHAPTER 4

IMPLEMENTATION

4.1 ENVIRONMENT SETUP

4.1.1 PYTHON 3.7.0 INSTALLATION

The following steps outline how to download and install Python 3.7.0:

Step 1) Visit the official Python website at python.org.Choose the appropriate installer for your Windows operating system architecture (32-bit or 64-bit).

Step 2) Once the installer is downloaded, locate the file in your Downloads folder. Double-click on the installer file (python-3.7.0-amd64.exe for 64-bit or python-3.7.0.exe for 32-bit) to launch the installation wizard.

Fig: 4.1 Python Setup Wizard

Step 3) In the Python Setup wizard, ensure that the option to "Add Python 3.7 to PATH" is selected. This option is crucial for allowing Python to be easily accessible from the command line. Click "Install Now" to proceed.

Step 4) Follow the prompts in the installation wizard to complete the installation process. The installer will copy necessary files and configure Python on your system. This may take a few minutes.

Step 5) After installation, open Command Prompt (Press Windows key + R type cmd, and press Enter to open Command Prompt). In the Command Prompt window, type the following command and press Enter: **python --version**

Step 6) You should see Python 3.7.0 (or a similar version number) displayed, confirming the successful installation of Python.

4.1.2 NODE.JS V12.13.1 INSTALLATION

The Following are the Node.js v12.13.1 Installation Steps for Windows:

Step 1) Navigate to the official Node.js website at https://nodejs.org/en/download/releases/. Download the Node.js v12.13.1 installer for Windows.

Step 2) Once the installer is downloaded, locate the file in your Downloads folder. Double-click on the downloaded installer file to run the installation wizard.

Step 3) During the installation process, you will be prompted to accept the license agreement. Read through the agreement and proceed by accepting it.

Step 4) In the installation wizard, you may encounter various options. Ensure that the option to add Node.js to the system PATH is selected for easier command-line usage.

Step 5) Follow the prompts in the installation wizard to complete the installation process. Once finished, Node.js v12.13.1 will be installed on your Windows system.

Installation of Required Python Packages and NLTK Packages

To Install the Required Python Packages:

- Locate the requirements.txt file containing a list of Python packages required for your project.
- Open Command Prompt (Windows). Navigate to the directory containing the requirements.txt file using the cd command.

- Execute the following command to install the required packages: **pip install -r requirements.txt**
- This command will automatically install all the Python packages listed in the requirements.txt file.

To Install NLTK Packages:

- Locate and double-click on the **installNLTK.bat** file included in your project.
- A window will appear with an option to download NLTK packages. Click on the "Download" button to initiate the installation process.
- Once the installation is complete, the window will turn green, indicating successful installation.
- You can then safely close the window and proceed with the next steps of your project.

Blockchain Data Security Implementation:

Utilizing Blockchain, each data record is stored as a tamper-proof block with a unique hash code. Verification of previous block hash codes ensures data integrity. Smart Contracts, coded in Solidity, facilitate data storage and retrieval on the Blockchain. This robust system secures user data effectively, enhancing trust and reliability.

SmartContract.sol

C: > Users > asrij > AppData > Local > Temp > 585d03bd-d8c1-4f6e-b655-cb38bd012304_Crime-Alert.rar.304 > Crime-Alert > SmartContract.sol

```
pragma solidity >= 0.8.11 <= 0.8.11;

contract SmartContract {
    string public userdetails;
    string public tips;

    //call this function to register user details data to Blockchain
    function setSignup(string memory ud) public {
       userdetails = ud;
    }
   //get register details
    function getSignup() public view returns (string memory) {
        return userdetails;
    }

    //call this function to save tips in Blockchain
    function setTips(string memory t) public {
      tips = t;
    }
   //get tip details
    function getTips() public view returns (string memory) {
        return tips;
    }

   constructor() public {
        userdetails="";
    tips="";
    }
}
```

Fig: 4.2 SmartContract.sol File

In above contract we have define function to save and get user and their TIP details and we need to deploy above contract in Ethereum tool using below steps

1) First go inside 'hello-eth/node-modules/bin' folder and then find and double click on 'runBlockchain.bat' file to start Ethereum tool and then will get below screen

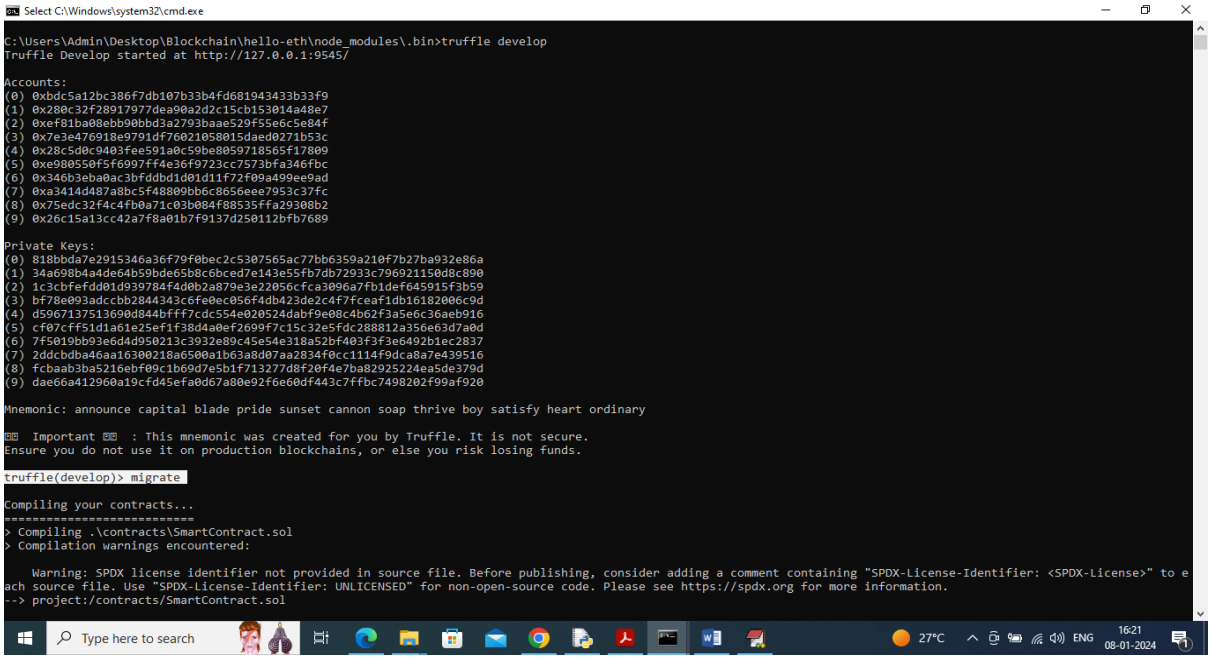


Fig: 4.3 Ethereum Startup

2) In above screen Ethereum tool started with default private keys and account and now type command as 'migrate' and press enter key to deploy contract and then will get below page

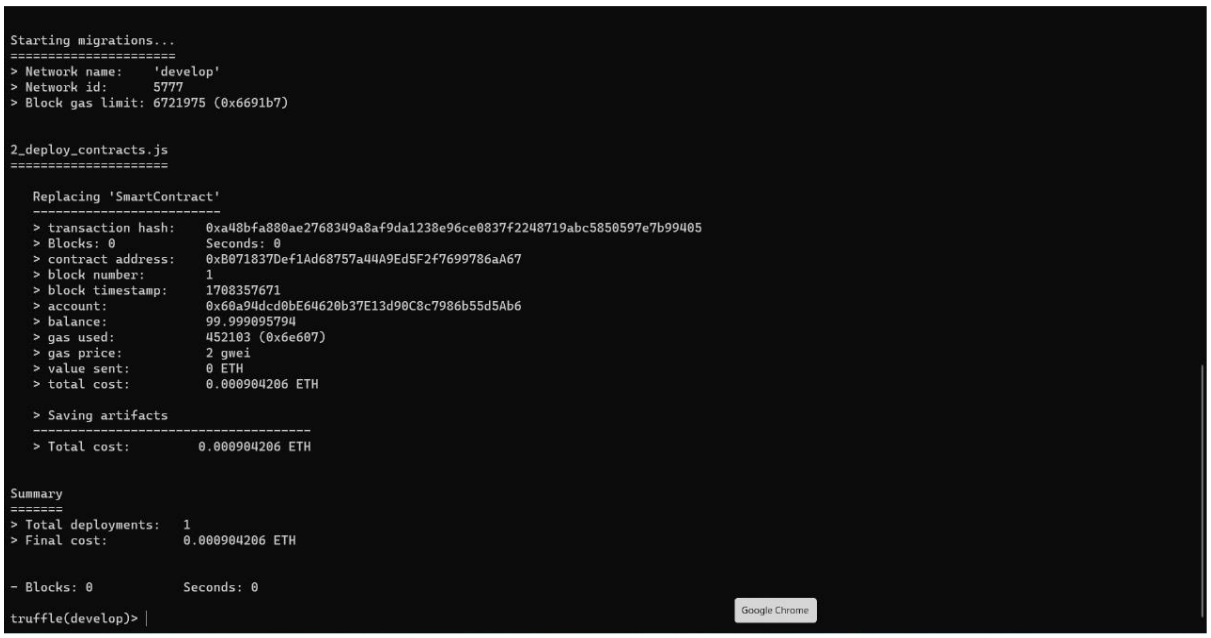


Fig: 4.4 Contract Deployed

3) In above screen we can see ‘Smart Contract’ deployed and got contract address also and this address need to specify in python code to save and get details from Ethereum and in below screen showing python code calling smart contract using

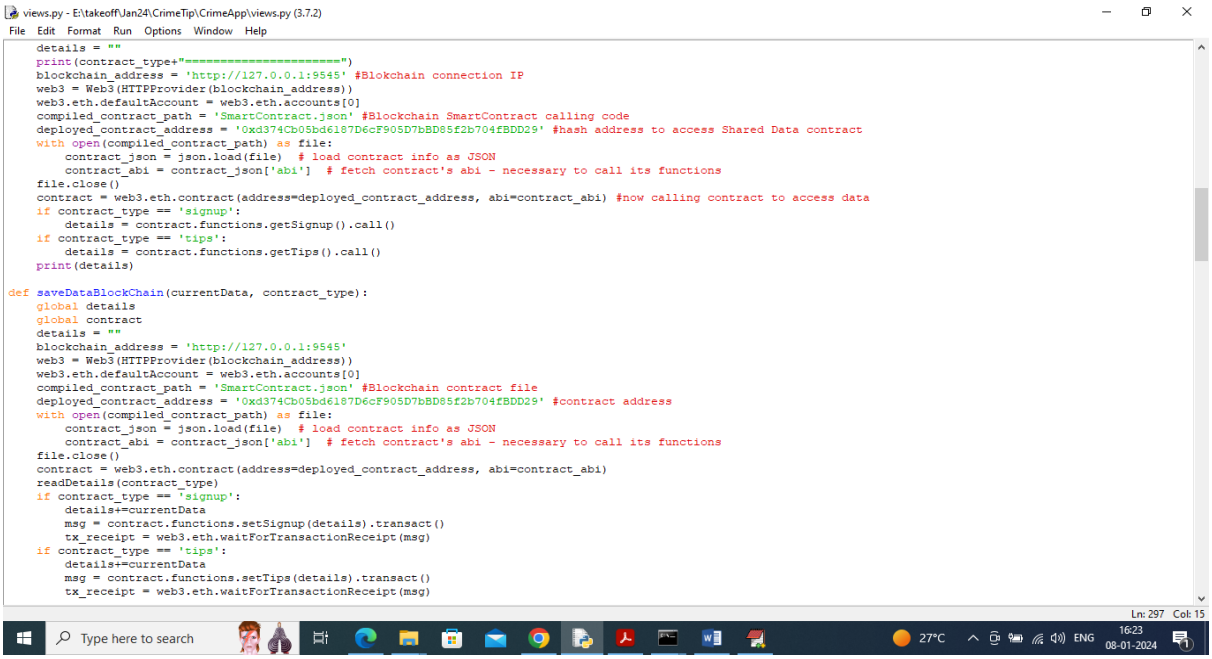


Fig: 4.5 Contract Calling

4) In above screen read red color comments to know about contract calling using python and now contract is deployed and let it run.

Data Storage and ML Algorithm Training:

IPFS for Multimedia Data Storage:

Utilize the IPFS (InterPlanetary File System) server to store multimedia data. Upon storage, retrieve a hash code representing the file location, which is then saved in the Blockchain. This hash code is subsequently employed for file retrieval from IPFS.

TIP Dataset for ML Algorithm:

Employ the TIP dataset for training the machine learning algorithm. The dataset comprises TIP descriptions, with the first-row denoting column names and subsequent rows representing dataset values. The final column indicates the class label, with '0' signifying a true 'Crime TIP Description' and '1' indicating false.

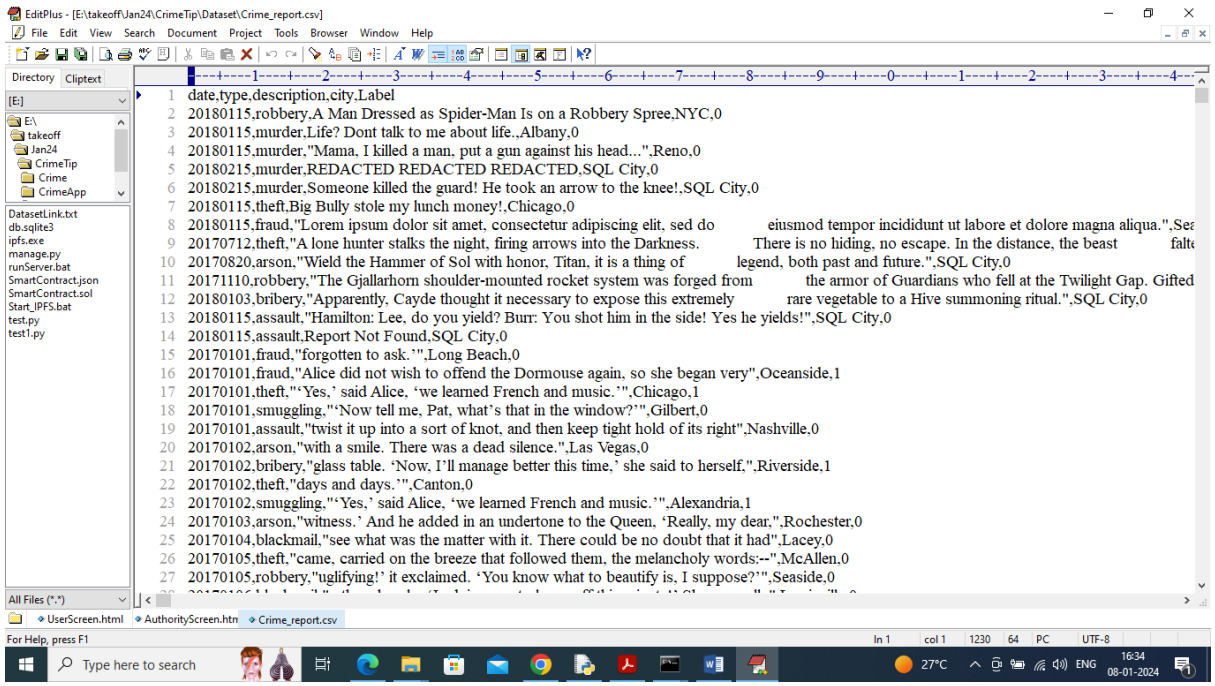


Fig: 4.6 Dataset Overview

In above dataset screen first row represents dataset column names and remaining rows represents dataset values and in last column we have class label as 0 and 1 where 0 means 'Crime TIP Description' is true and 1 means False.

Steps For Executing the Project:

1. To run project first double, click on 'runIPFS.bat' file to start IPFS server and get below page

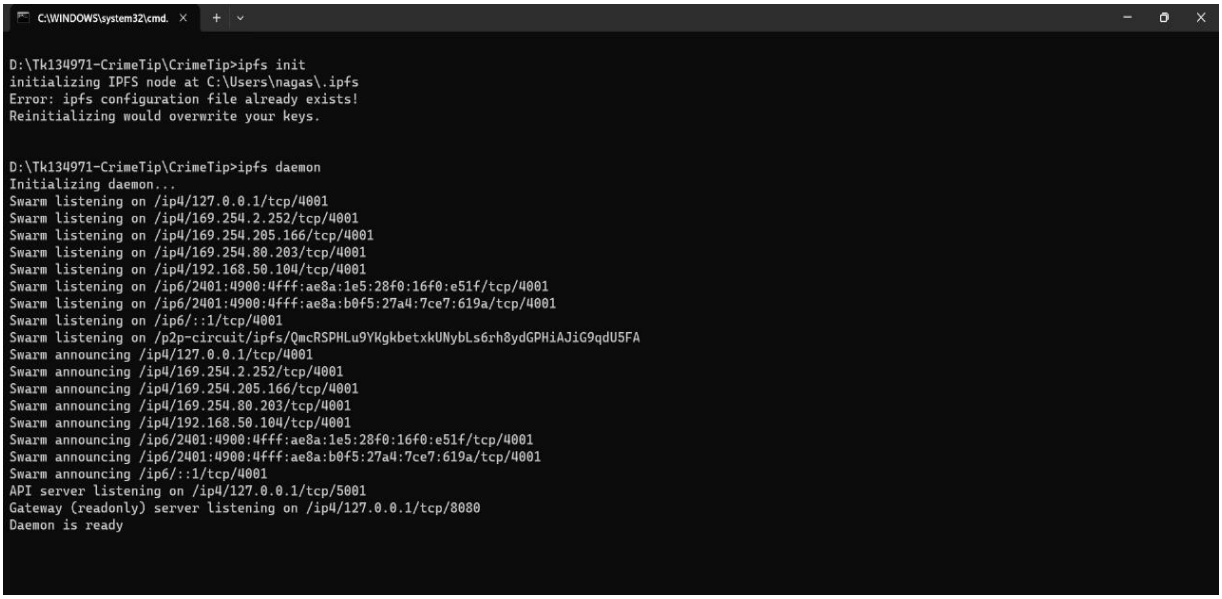


Fig: 4.7 IPFS Startup

2. In above screen IPFS server started and now double click on ‘runServer.bat’ file to start python web server and will get below page

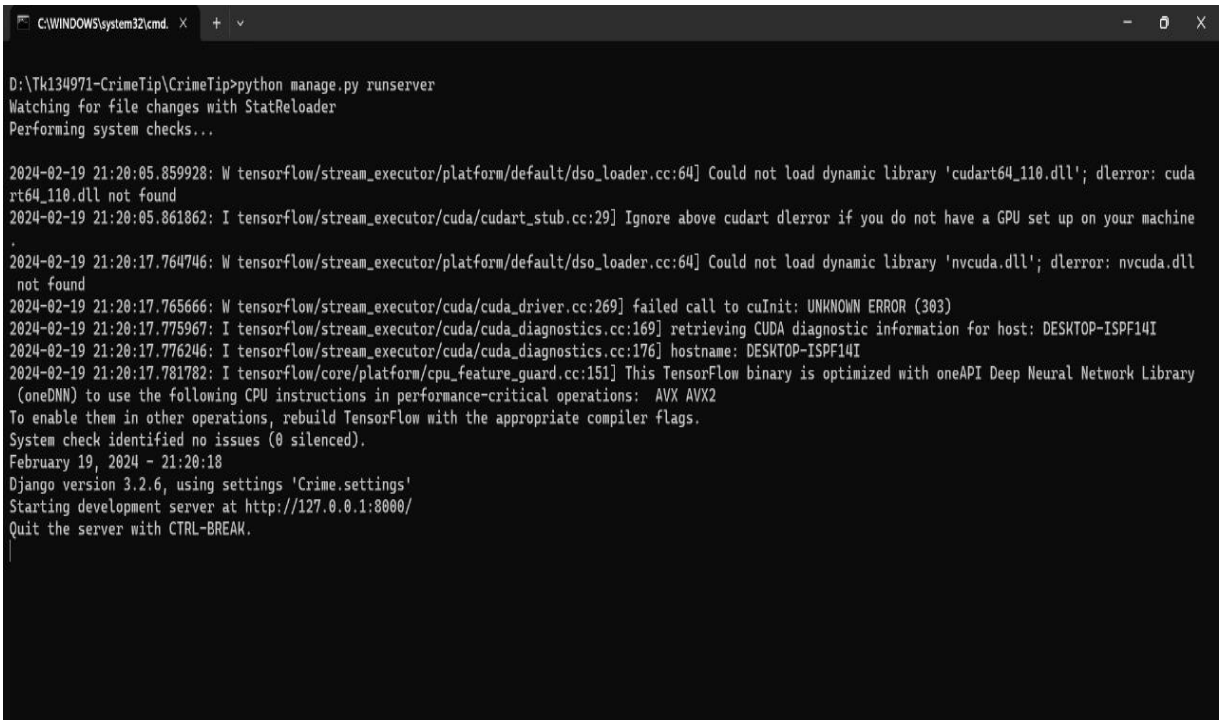


Fig: 4.8 Python Webserver Startup

3. In above screen python web server started and now open browser and enter URL as http://127.0.0.1:8000/ to access the Crime Alert Web Application.

CHAPTER 5

RESULT

In our Crime Alert: An Anonymous Crime Reporting System project, anonymity and confidentiality within the system are ensured through the implementation of a **unique ID generation** mechanism. Each crime report is assigned a distinct identifier, safeguarding the identities of both reporters and subjects involved in reported incidents. This anonymity protection fosters a secure environment for reporting sensitive information without fear of retribution or exposure.

Fig:5.1 Unique Id Generation

And The implementation of **TensorFlow CNN algorithm** efficiently preprocesses text data, performs word embedding, and partitions data for training, validation, and testing. The trained model accurately distinguishes between true and false crime reports, enhancing the reliability and effectiveness of our Crime Alert system.

Username	Suspicious Activity Address	Type of Activity	Tip Description	Hashcode	Tip Date	Predicted Report Status	Tip Image
vishnu	near SBI ATM, Prathipadu, Guntur, AP	Murder	Murder near my home, someone has been murdered. The criminal has curl hair, around 5.5 height, fair skinned with mask on face and had bracelets on hand	QmTgSvUVQUHU7W12uGxfhkG2eFGQtmT7kdGhCb6akCt3oi	2024-03-16 09:48:28	True Report Predicted	

Fig:5.2 Prediction of the crime report

The model achieves an exceptional accuracy rate of 99.19%, indicating its proficiency in correctly classifying crime reports as true or false. This high accuracy demonstrates the reliability of the system in distinguishing between genuine incidents and false alarms, thereby enhancing the credibility of reported information.

With a precision score of 96.46%, the system exhibits a low false positive rate, accurately identifying true crime reports while minimizing misclassifications. High precision ensures that legitimate incidents are effectively recognized and acted upon, reducing the likelihood of erroneous conclusions or responses.

The recall score of 199.45% signifies the system's capability to capture a significant portion of true crime reports among all actual positive instances. This high recall rate reflects the system's sensitivity to identifying genuine incidents, thereby maximizing the coverage of reported crimes and facilitating appropriate intervention measures.

Algorithm Name	Accuracy	Precision	Recall	FScore
Tensorflow CNN Algorithm	0.991869918699187	98.46153846153847	99.4535519125683	98.94402472527473

Fig:5.3 TensorFlow CNN Metrics

The F1 score, calculated at 98.94%, represents a harmonized measure of the system's precision and recall performance. This balanced evaluation metric underscores the system's effectiveness in simultaneously achieving high precision and recall, ensuring robustness and reliability in crime report classification.

5.1 OUTPUT SCREENS

Modules

New User Sign up: using this module user can sign up with the application

User Login: using this module user can login to application and all user details will be managed with server in AES encrypted format

Submit your Tip: after login using this module user can submit tip about any suspicious activities

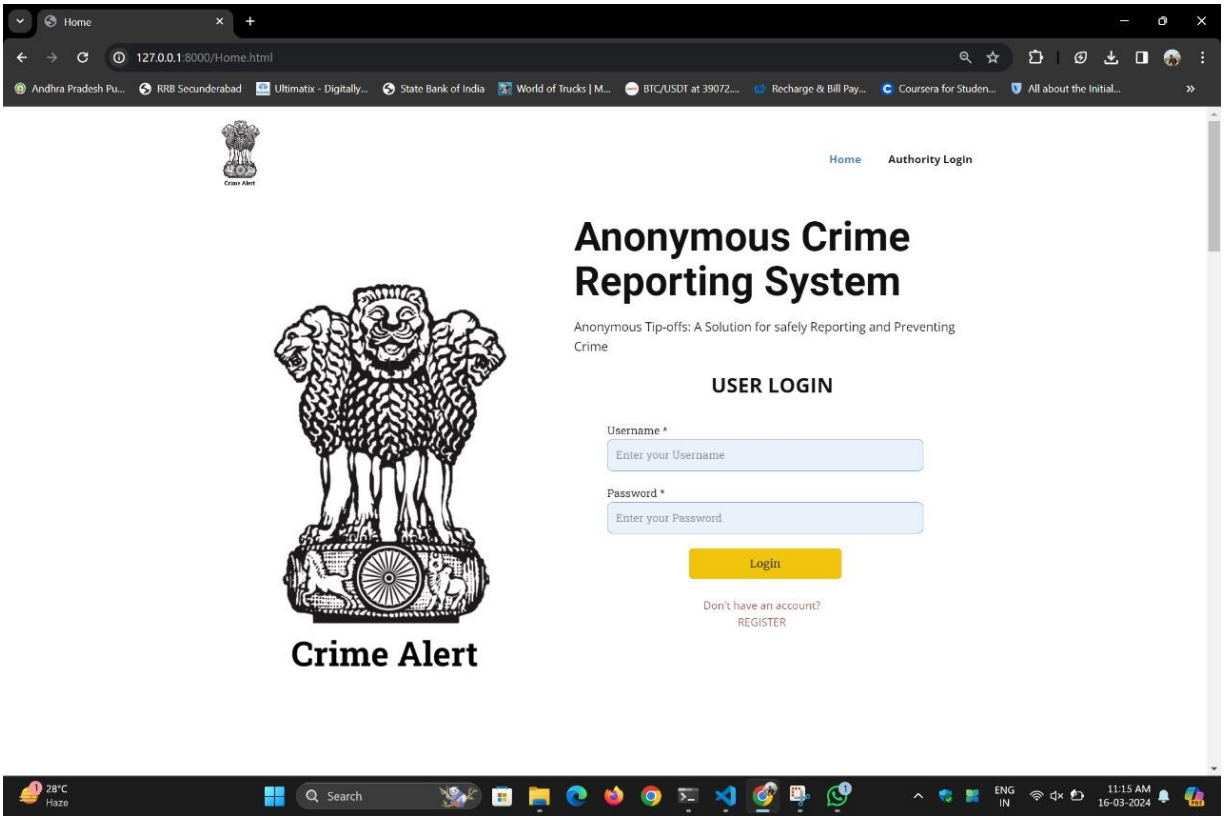
View your Past Tips: using this module user can view all submitted tip reports

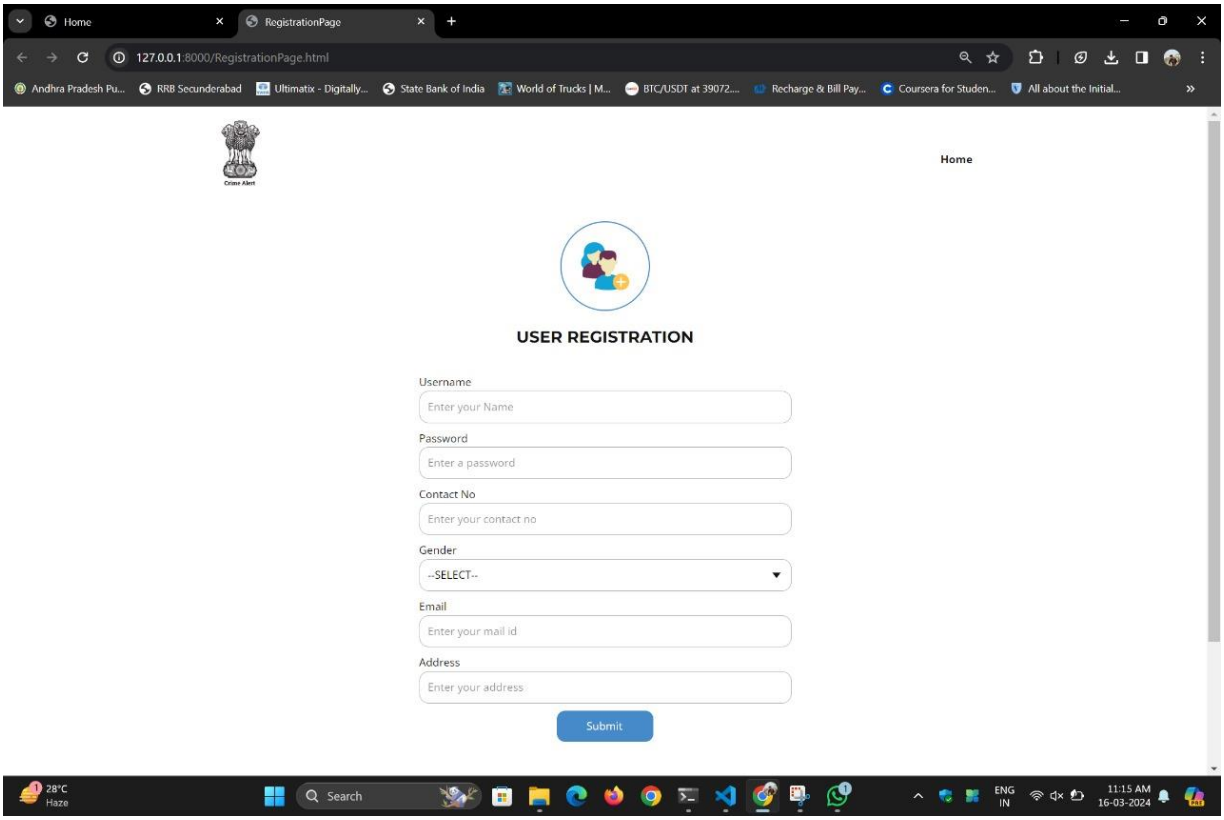
Authority Login: authority can login to system using username and password as ‘admin’. After login authority can perform following options

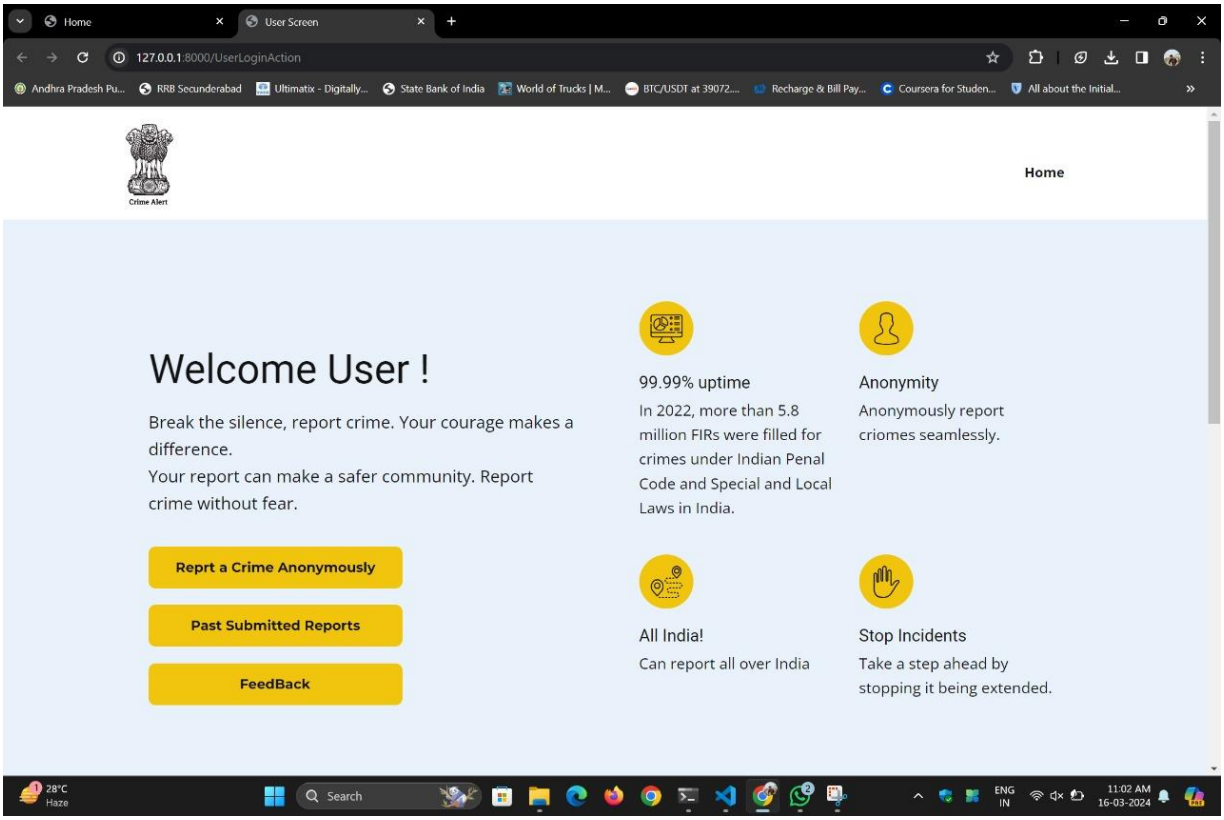
Train ML: using this module authority can train ML to predict weather submitted tip is false or true

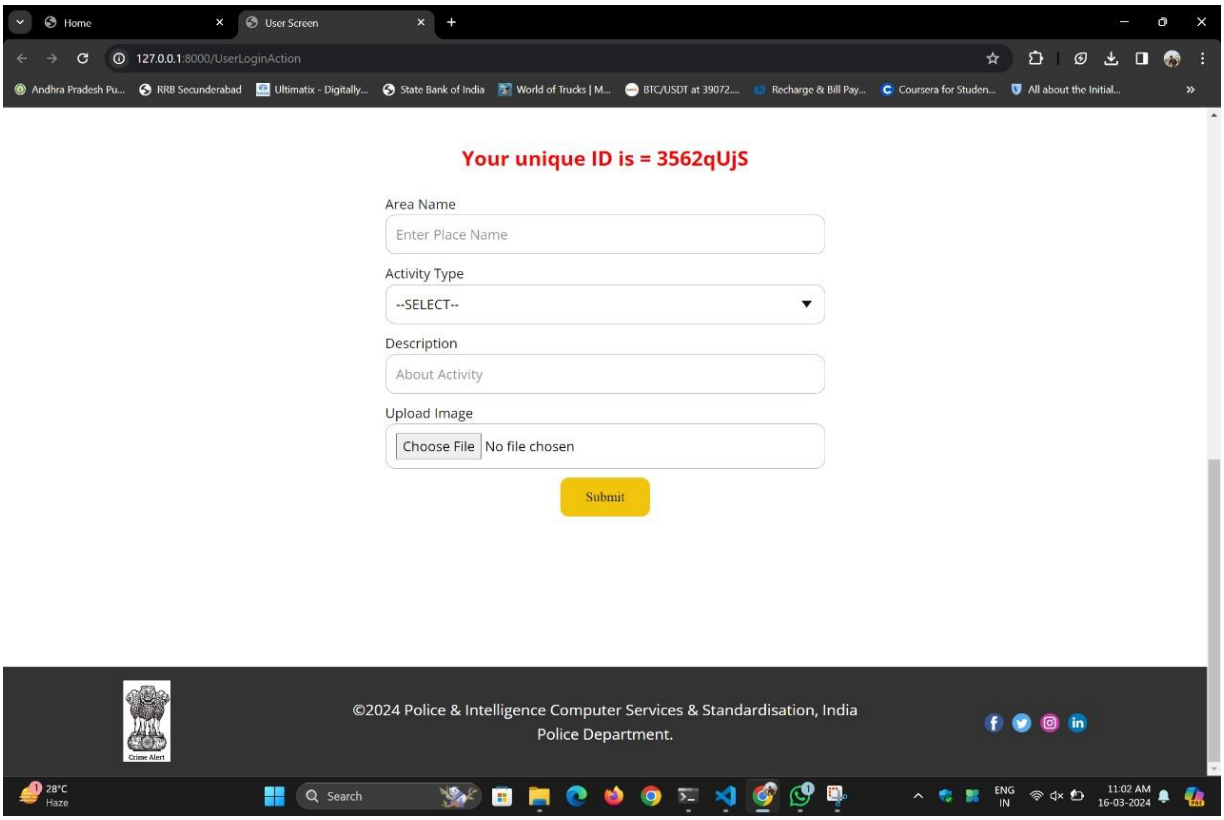
View Submitted Tips Report: using this module authority can view all submitted tips and machine learning predicted top status as true or false

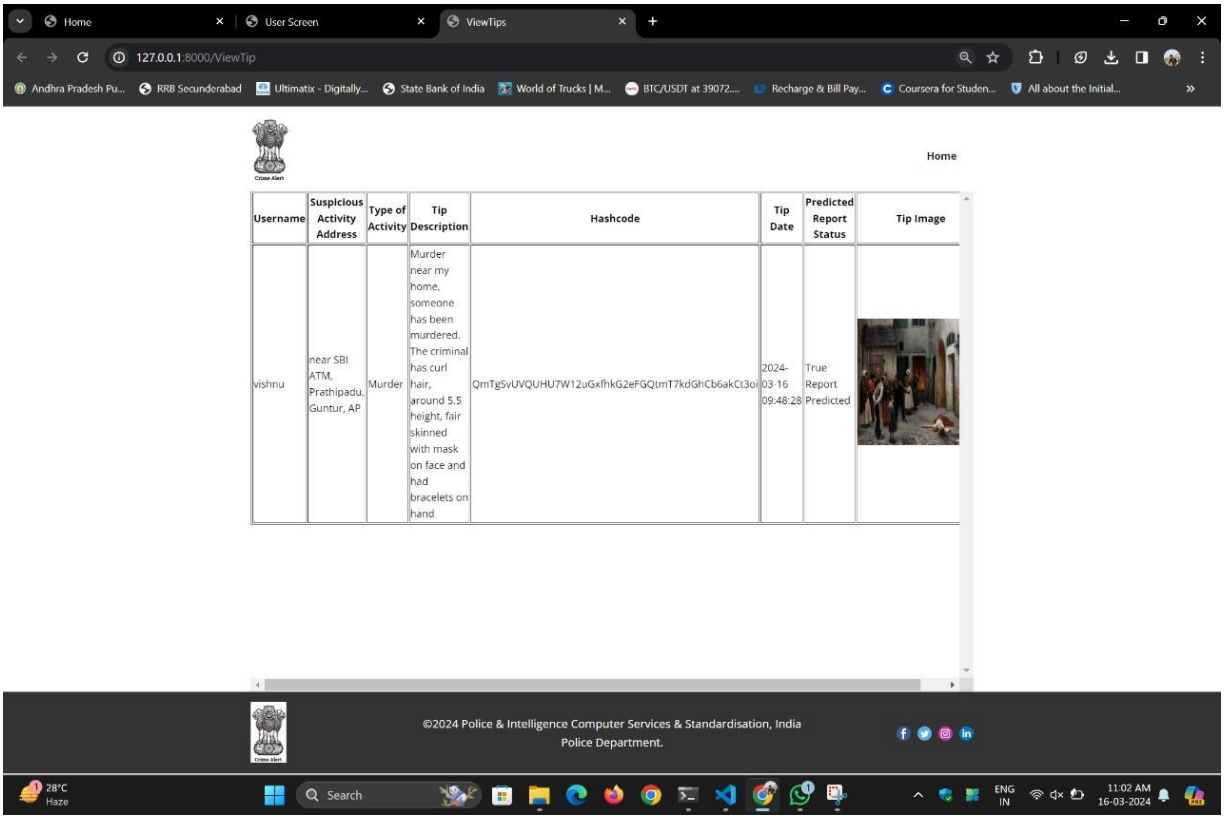
View User Lists: using this module authority can view all registered user details but all username will be anonymised for security reason

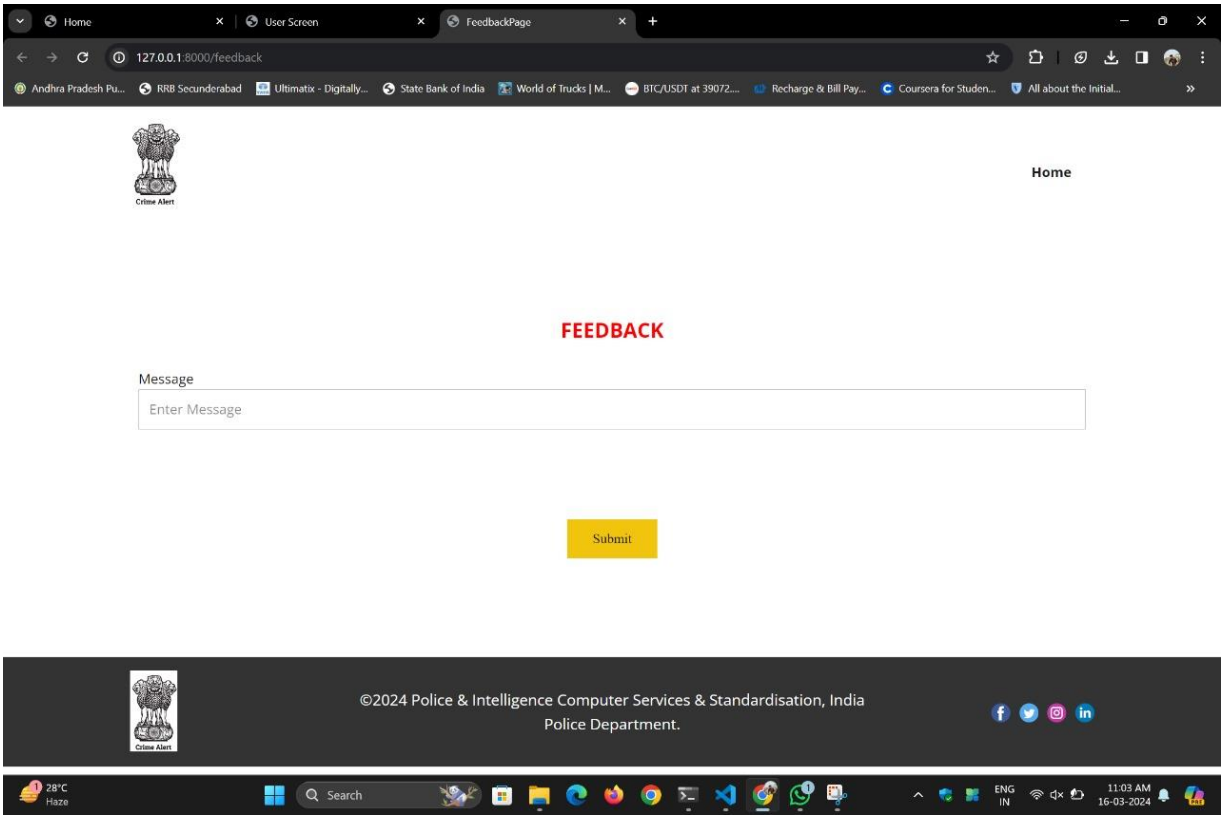

Home
127.0.0.1:8000/Home.html
Andhra Pradesh Pu...
RRB Secunderabad
Ultimatix - Digitally...
State Bank of India
World of Trucks | M...
BTC/USDT at 39072....
Recharge & Bill Pay...
Coursera for Studen...
All about the Initial...
Home
Authority Login
Anonymous Crime Reporting System
Anonymous Tip-offs: A Solution for safely Reporting and Preventing Crime
USER LOGIN
Username *
Enter your Username
Password *
Enter your Password
Login
Don't have an account?
REGISTER
Crime Alert
28°C
Haze
Search
ENG
IN
11:15 AM
16-03-2024

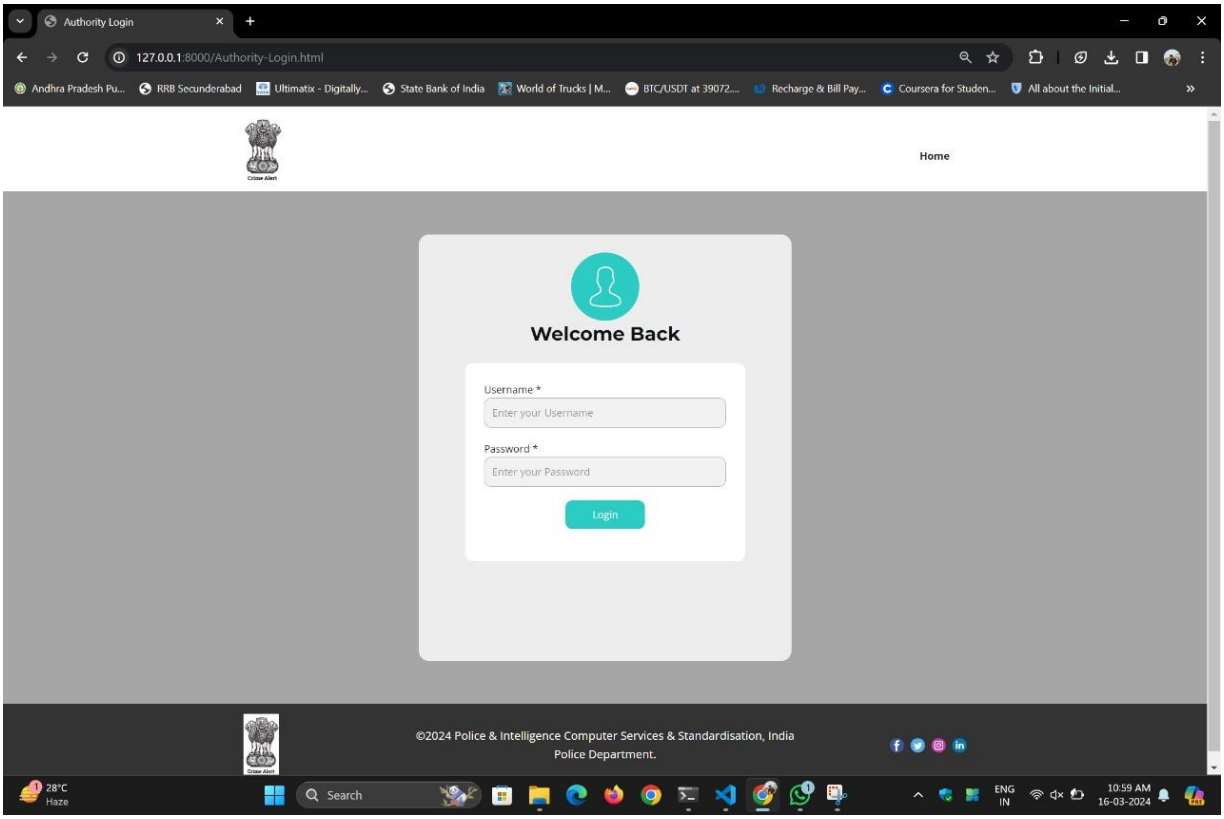

Home
RegistrationPage
127.0.0.1:8000/RegistrationPage.html
Andhra Pradesh Pu...
RRB Secunderabad
Ultimatix - Digitally...
State Bank of India
World of Trucks | M...
BTC/USDT at 39072....
Recharge & Bill Pay...
Coursera for Studen...
All about the Initial...
Crime Alert
Home
USER REGISTRATION
Username
Enter your Name
Password
Enter a password
Contact No
Enter your contact no
Gender
--SELECT--
Email
Enter your mail id
Address
Enter your address
Submit
28°C
Haze
Search
ENG
IN
11:15 AM
16-03-2024

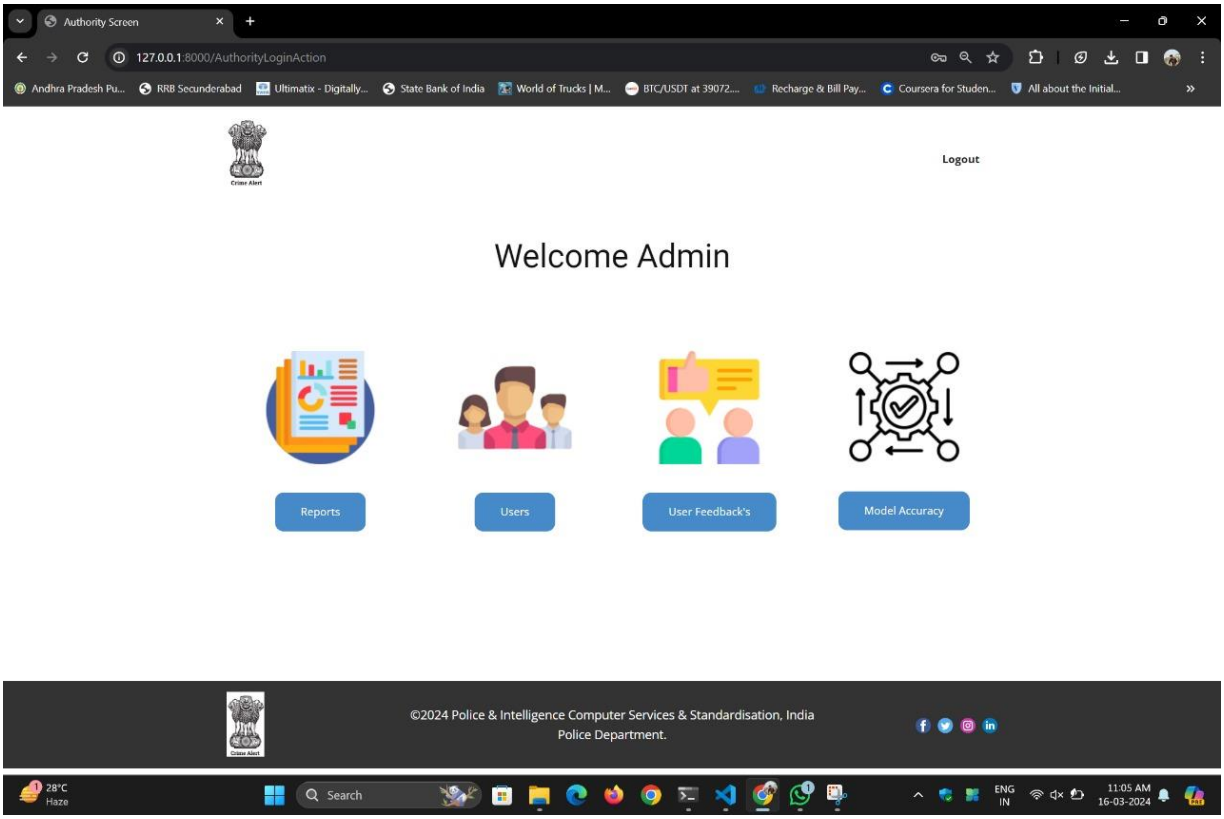

Home
User Screen
127.0.0.1:8000/UserLoginAction
Andhra Pradesh Pu...
RRB Secunderabad
Ultimatix - Digitally...
State Bank of India
World of Trucks | M...
BTC/USDT at 39072....
Recharge & Bill Pay...
Coursera for Studen...
All about the Initial...
Crime Alert
Home
Welcome User !
Break the silence, report crime. Your courage makes a difference.
Your report can make a safer community. Report crime without fear.
Reprt a Crime Anonymously
Past Submitted Reports
FeedBack
99.99% uptime
In 2022, more than 5.8 million FIRs were filled for crimes under Indian Penal Code and Special and Local Laws in India.
Anonymity
Anonymously report criomes seamlessly.
All India!
Can report all over India
Stop Incidents
Take a step ahead by stopping it being extended.
28°C
Haze
Search
ENG
IN
11:02 AM
16-03-2024

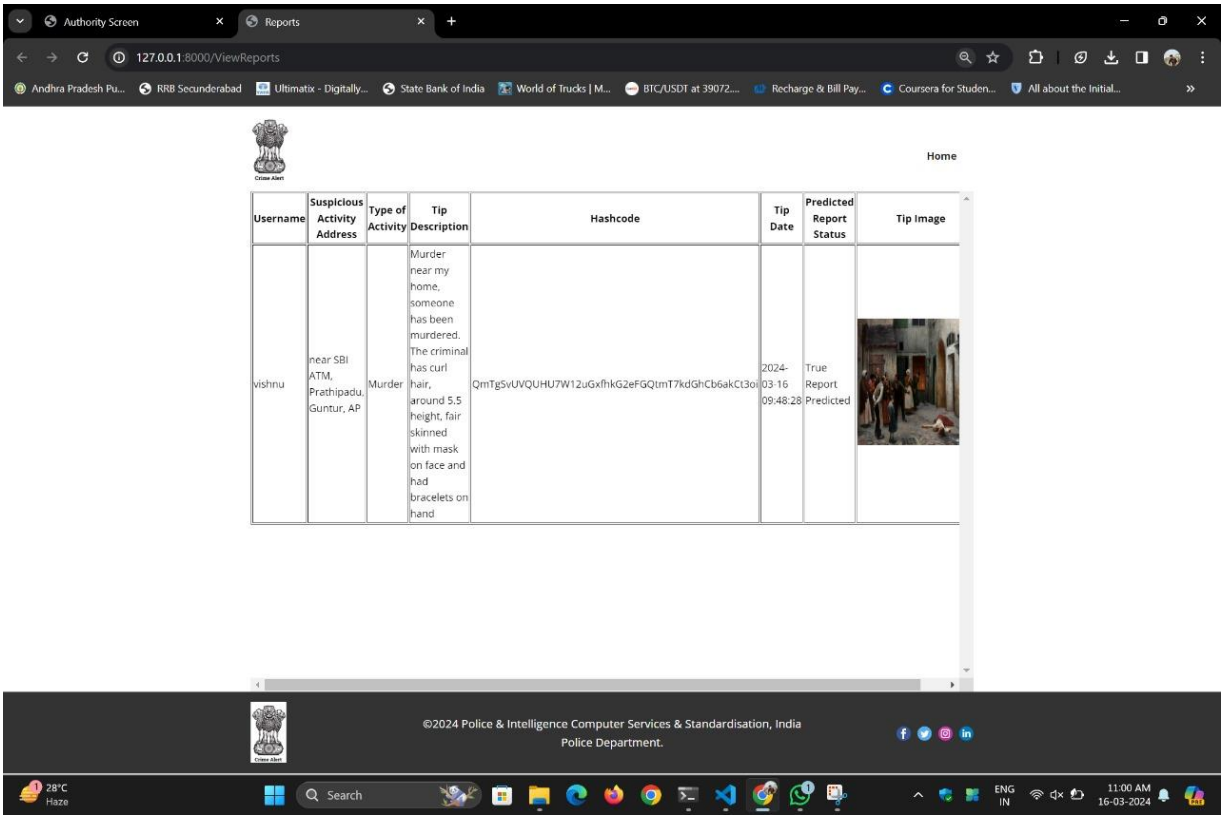

Home
User Screen
127.0.0.1:8000/UserLoginAction
Andhra Pradesh Pu...
RRB Secunderabad
Ultimatix - Digitally...
State Bank of India
World of Trucks | M...
BTC/USDT at 39072....
Recharge & Bill Pay...
Coursera for Studen...
All about the Initial...
Your unique ID is = 3562qUjS
Area Name
Enter Place Name
Activity Type
--SELECT--
Description
About Activity
Upload Image
Choose File
No file chosen
Submit
Crime Alert
©2024 Police & Intelligence Computer Services & Standardisation, India Police Department.
28°C
Haze
Search
ENG
IN
11:02 AM
16-03-2024

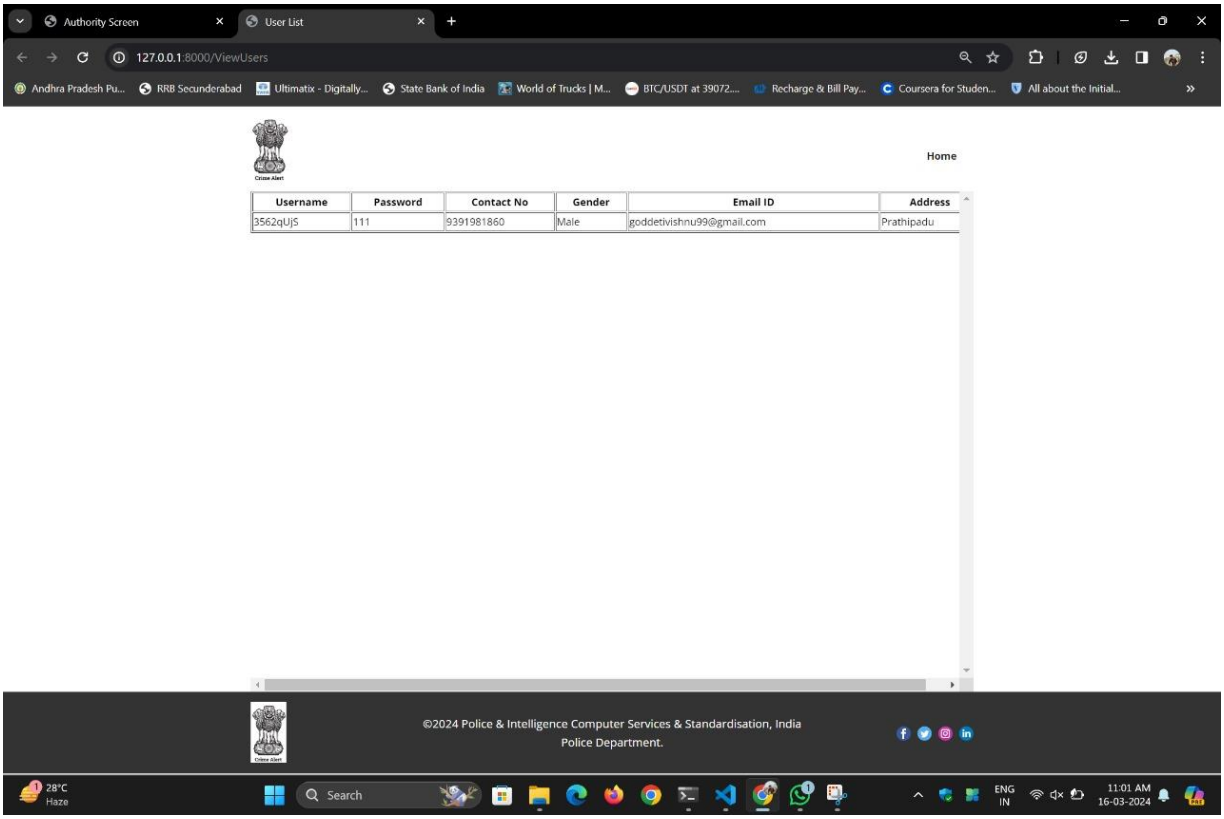

Home
User Screen
ViewTips
127.0.0.1:8000/ViewTip
Andhra Pradesh Pu...
RRB Secunderabad
Ultimatix - Digitally...
State Bank of India
World of Trucks | M...
BTC/USDT at 39072....
Recharge & Bill Pay...
Coursera for Studen...
All about the Initial...
Crime Alert
Home
Username
Suspicious Activity Address
Type of Activity
Tip Description
Hashcode
Tip Date
Predicted Report Status
Tip Image
vishnu
near SBI ATM, Prathipadu, Guntur, AP
Murder
Murder near my home, someone has been murdered. The criminal has curl hair, around 5.5 height, fair skinned with mask on face and had bracelets on hand
QmTgSvUVQUHU7W12uGxfhkG2eFGQtmT7kdGhCb6akCt3oi
2024-03-16 09:48:28
True Report Predicted
©2024 Police & Intelligence Computer Services & Standardisation, India Police Department.
28°C Haze
Search
ENG IN
11:02 AM 16-03-2024

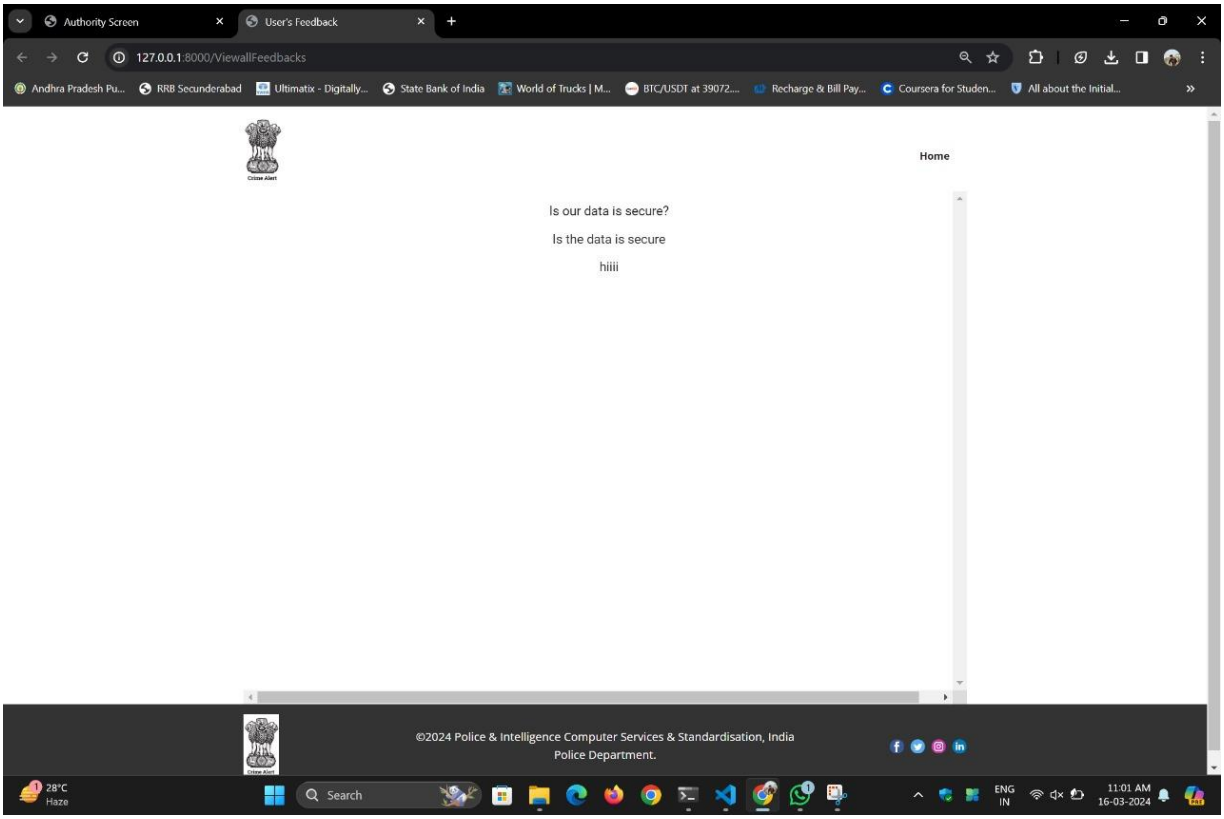

Home
User Screen
FeedbackPage
127.0.0.1:8000/feedback
Andhra Pradesh Pu...
RRB Secunderabad
Ultimatix - Digitally...
State Bank of India
World of Trucks | M...
BTC/USDT at 39072....
Recharge & Bill Pay...
Coursera for Studen...
All about the Initial...
Crime Alert
Home
FEEDBACK
Message
Enter Message
Submit
Crime Alert
©2024 Police & Intelligence Computer Services & Standardisation, India Police Department.
28°C
Haze
Search
ENG
IN
11:03 AM
16-03-2024

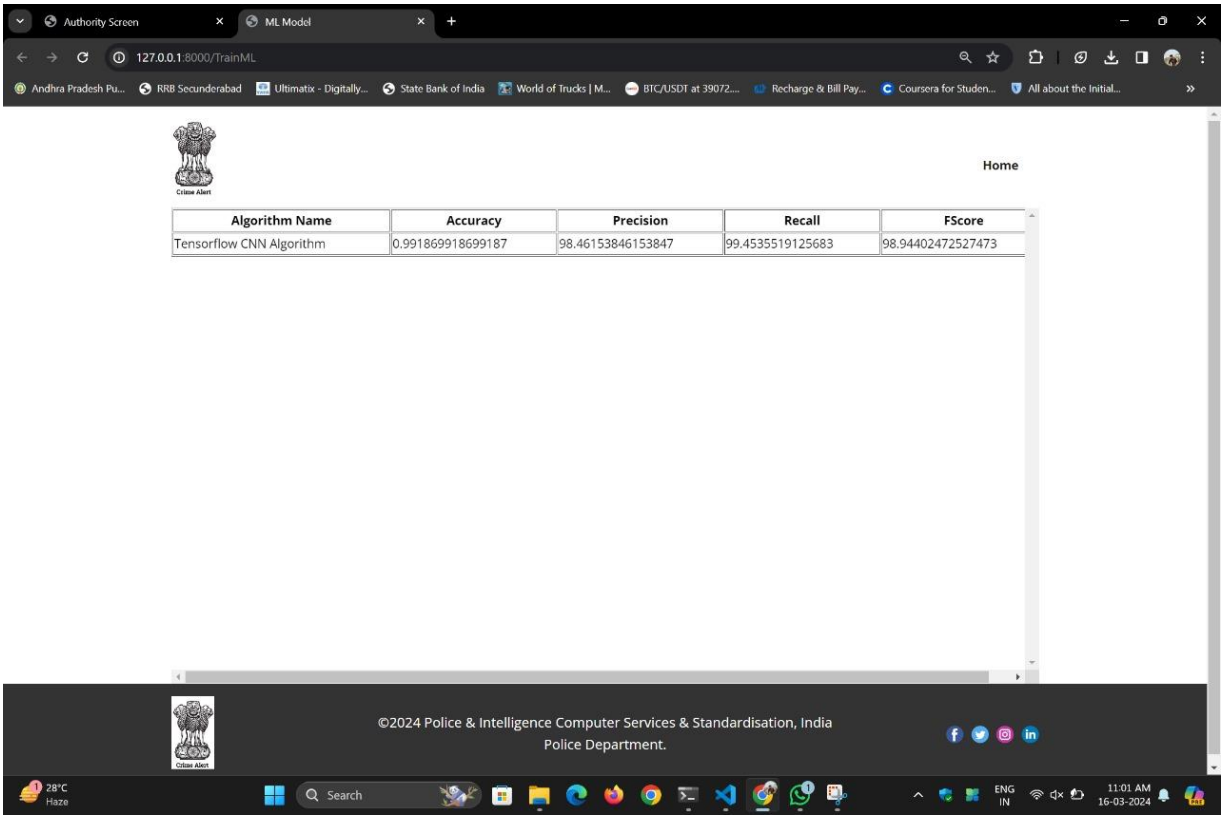

Authority Login
127.0.0.1:8000/Authority-Login.html
Andhra Pradesh Pu...
RRB Secunderabad
Ultimatix - Digitally...
State Bank of India
World of Trucks | M...
BTC/USDT at 39072....
Recharge & Bill Pay...
Coursera for Studen...
All about the Initial...
Home
Welcome Back
Username *
Enter your Username
Password *
Enter your Password
Login
©2024 Police & Intelligence Computer Services & Standardisation, India
Police Department.
28°C
Haze
Search
ENG
IN
10:59 AM
16-03-2024


Authority Screen
127.0.0.1:8000/AuthorityLoginAction
Andhra Pradesh Pu...
RRB Secunderabad
Ultimatix - Digitally...
State Bank of India
World of Trucks | M...
BTC/USDT at 39072....
Recharge & Bill Pay...
Coursera for Studen...
All about the Initial...
Logout
Welcome Admin
Reports
Users
User Feedback's
Model Accuracy
©2024 Police & Intelligence Computer Services & Standardisation, India Police Department.
28°C
Haze
Search
ENG
IN
11:05 AM
16-03-2024


Authority Screen
Reports
127.0.0.1:8000/ViewReports
Andhra Pradesh Pu...
RRB Secunderabad
Ultimatix - Digitally...
State Bank of India
World of Trucks | M...
BTC/USDT at 39072....
Recharge & Bill Pay...
Coursera for Studen...
All about the Initial...
Home
Username
Suspicious Activity Address
Type of Activity
Tip Description
Hashcode
Tip Date
Predicted Report Status
Tip Image
vishnu
near SBI ATM, Prathipadu, Guntur, AP
Murder
Murder near my home, someone has been murdered. The criminal has curl hair, around 5.5 height, fair skinned with mask on face and had bracelets on hand
QmTgSvUVQUHU7W12uGxfhkG2eFGQtmT7kdGhCb6akCt3oi
2024-03-16 09:48:28
True Report Predicted
©2024 Police & Intelligence Computer Services & Standardisation, India Police Department.
28°C Haze
Search
ENG IN
11:00 AM 16-03-2024


Authority Screen
User List
127.0.0.1:8000/ViewUsers
Andhra Pradesh Pu...
RRB Secunderabad
Ultimatix - Digitally...
State Bank of India
World of Trucks | M...
BTC/USDT at 39072....
Recharge & Bill Pay...
Coursera for Studen...
All about the Initial...
Home
Username
Password
Contact No
Gender
Email ID
Address
3562qUjS
111
9391981860
Male
goddetivishnu99@gmail.com
Prathipadu
©2024 Police & Intelligence Computer Services & Standardisation, India
Police Department.
28°C
Haze
Search
ENG
IN
11:01 AM
16-03-2024


Authority Screen
User's Feedback
127.0.0.1:8000/ViewallFeedbacks
Andhra Pradesh Pu...
RRB Secunderabad
Ultimatix - Digitally...
State Bank of India
World of Trucks | M...
BTC/USDT at 39072....
Recharge & Bill Pay...
Coursera for Studen...
All about the Initial...
Home
Is our data is secure?
Is the data is secure
hiiii
©2024 Police & Intelligence Computer Services & Standardisation, India
Police Department.
28°C
Haze
Search
ENG
IN
11:01 AM
16-03-2024


Authority Screen
ML Model
127.0.0.1:8000/TrainML
Andhra Pradesh Pu...
RRB Secunderabad
Ultimatix - Digitally...
State Bank of India
World of Trucks | M...
BTC/USDT at 39072....
Recharge & Bill Pay...
Coursera for Studen...
All about the Initial...
Crime Alert
Home
Algorithm Name
Accuracy
Precision
Recall
FScore
Tensorflow CNN Algorithm
0.991869918699187
98.46153846153847
99.4535519125683
98.94402472527473
Crime Alert
©2024 Police & Intelligence Computer Services & Standardisation, India
Police Department.
28°C
Haze
Search
ENG
IN
11:01 AM
16-03-2024

CHAPTER 6

CONCLUSION AND FUTURE SCOPRE

The Crime Alert: An Anonymous Crime Reporting System project signifies a significant stride in simplifying and securing the reporting of crimes. Utilizing advanced technologies such as Convolutional Neural Networks and Blockchain Ethereum, it ensures that individuals can report criminal activities without fear of their safety or privacy being compromised.

The primary aim is to establish a safe platform where whistleblowers and witnesses can speak up without the threat of retaliation. Additionally, it assists law enforcement agencies in better understanding and responding to reported crimes through data analysis. By employing sophisticated algorithms and secure record-keeping methods, the Crime Alert system provides a reliable means of categorizing and tracking reported incidents, fostering trust between users and authorities and promoting transparency and accountability in the reporting process. Prioritizing user anonymity and data integrity, the project promotes a culture of community safety and collaboration, demonstrating how technology can be harnessed for positive social impact.

The future development of the Crime Alert: An Anonymous Crime Reporting System aims to enhance user empowerment and refine analytical capabilities. One significant enhancement is the integration of AI-powered chatbots to streamline the reporting process, making it more accessible and engaging.

Furthermore, incorporating multi-modal reporting options such as mobile apps and SMS promotes inclusivity and ensures widespread participation, accommodating diverse user preferences and accessibility needs. Additionally, the system will leverage Natural Language Processing (NLP) algorithms to extract deeper insights from reported data, enabling a more nuanced understanding of the information provided. Integration of decentralized identity verification systems will strengthen user anonymity while preserving data integrity, enhancing user confidence and the reliability of reported information. These enhancements reflect Crime Alert's commitment to continuous improvement, striving to enhance efficiency, accessibility, and accuracy in handling reported incidents, ultimately contributing to the creation of safer and more secure communities.

CHAPTER -7

REFERENCES

[1]. Yao Du, Shuxiao Miao, Zitian Tong, Victoria Lemieux & Zehua Wang "Blockchain-Empowered Mobile Edge Intelligence, Machine Learning and Secure Data Sharing" - March 2021

[2]. Vishal A. Kharde & S.S. Sonawane, "Sentiment Analysis of Twitter Data: A Survey of Techniques" - April 2016

[3]. Jasleen Kaur and Dr. Jatinderkumar R. Saini "A Study of Text Classification Natural Language Processing Algorithms for Indian Languages" - – July 2015

[4]. ArcharnaM, Durga S, Saveetha K "Online Crime Reporting System"

[5]. Riya Lohan and Mr.Mahesh Singth, " An Online Crime Reporting System" – Research Paper-June 2015

[6] B. Holtmann, and Domingo-Swarts, "Current trends and responses to crime in South Africa. Crime," Violence and Injury Prevention in South Africa, 2008, pp 105 - 129.

[7] G. Paula, "Crime-fighting sensors." Mechanical Engineering Magazine Select Articles, 120 (01), 1998. pp.66-68.

[8] Kovács, L., Szlávik, Z., Benedek, C., Havasi, L., Petrás, I., Losteiner, D., Utasi, Á., Liscár, A., Czúni, L. and Szirányi, T., "Video Surveillance Framework for Crime Prevention and Event Indexing," in ICT4Justice, January 2008.

[9] H. Van Vuuren, "Small bribes big challenge: Extent and nature of petty corruption SouthAfrica" South African Crime Quarterly, (9), 2004.

[10] Diva Lal, Adiba Abidin, Naveen Garg, and Vikas Deep. "Advanced immediate crime reporting to police in India." Procedia Computer Science, 85:543–549, 2016.

[11] Tzay-Farn Shih, Chin-Ling Chen, Bo-Yan Syu, andYong-Yuan Deng. A cloud-based crime reporting system with identity protection. Symmetry, 11(2):255, 2019.

APPENDIX

Published Article Certificates


International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Referred, Scholarly Indexed, Open Access Journal Since 2013)

IJIRCCE

Impact Factor 8.379

CERTIFICATE

OF PUBLICATION

The Board of IJIRCCE is hereby awarding this certificate to

GNANENDRA K

Assistant Professor, Department of CSE(AI&ML), Vasireddy Venkatadri Institute of Technology, Guntur, A.P., India

in Recognition of publication of the paper entitled

"Crime Alert: Anonymous Crime Reporting System"

in IJIRCCE, Volume 12, Issue 3, March 2024

Google scholar Crossref Mendeley doi INNO SPACE SJIF Scientific Journal Impact Factor

e-ISSN: 2320-9801
p-ISSN: 2320-9798

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Editor-in-Chief

www.ijircce.com ijircce@gmail.com

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Referred, Scholarly Indexed, Open Access Journal Since 2013)

IJIRCCE

Impact Factor 8.379

CERTIFICATE

OF PUBLICATION

The Board of IJIRCCE is hereby awarding this certificate to

NAGASIVANI N

Department of CSE(AI&ML), Vasireddy Venkatadri Institute of Technology, Guntur, A.P., India

in Recognition of publication of the paper entitled

"Crime Alert: Anonymous Crime Reporting System "

in IJIRCCE, Volume 12, Issue 3, March 2024

Google scholar Crossref Mendeley doi INNO SPACE SJIF Scientific Journal Impact Factor

e-ISSN: 2320-9801
p-ISSN: 2320-9798

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Editor-in-Chief

www.ijircce.com ijircce@gmail.com

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Referred, Scholarly Indexed, Open Access Journal Since 2013)

IJIRCCE

Impact Factor 8.379

CERTIFICATE

OF PUBLICATION

The Board of IJIRCCE is hereby awarding this certificate to

SRIJA REDDY A

Department of CSE(AI&ML), Vasireddy Venkatadri Institute of Technology, Guntur, A.P., India

in Recognition of publication of the paper entitled

"Crime Alert: Anonymous Crime Reporting System "

in IJIRCCE, Volume 12, Issue 3, March 2024

Google scholar · Crossref · Mendeley · doi · INNO SPACE SJIF Scientific Journal Impact Factor

e-ISSN: 2320-9801
p-ISSN: 2320-9798

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Editor-in-Chief

www.ijircce.com ijircce@gmail.com

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Referred, Scholarly Indexed, Open Access Journal Since 2013)

IJIRCCE

Impact Factor 8.379

CERTIFICATE

OF PUBLICATION

The Board of IJIRCCE is hereby awarding this certificate to

NAGA SUNDEEP M

Department of CSE(AI&ML), Vasireddy Venkatadri Institute of Technology, Guntur, A.P., India

in Recognition of publication of the paper entitled

"Crime Alert: Anonymous Crime Reporting System "

in IJIRCCE, Volume 12, Issue 3, March 2024

Google scholar · Crossref · Mendeley · doi · INNO SPACE SJIF Scientific Journal Impact Factor

e-ISSN: 2320-9801
p-ISSN: 2320-9798

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Editor-in-Chief

www.ijircce.com ijircce@gmail.com

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Referred, Scholarly Indexed, Open Access Journal Since 2013)

CERTIFICATE

OF PUBLICATION

The Board of IJIRCCE is hereby awarding this certificate to

VISHNU CHAITANYA G

Department of CSE(AI&ML), Vasireddy Venkatadri Institute of Technology, Guntur, A.P., India

in Recognition of publication of the paper entitled

"Crime Alert: Anonymous Crime Reporting System "

in IJIRCCE, Volume 12, Issue 3, March 2024

e-ISSN: 2320-9801
p-ISSN: 2320-9798

www.ijircce.com ijircce@gmail.com

Published Article in the Journal

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203109 |

Crime Alert: Anonymous Crime Reporting System

Nagasivani N, Srija Reddy A, Naga Sundeep M, Vishnu Chaitanya G, Gnanendra K

Department of CSE(AI&ML), Vasireddy Venkatadri Institute of Technology, Guntur, A.P., India

Department of CSE(AI&ML), Vasireddy Venkatadri Institute of Technology, Guntur, A.P., India

Department of CSE(AI&ML), Vasireddy Venkatadri Institute of Technology, Guntur, A.P., India

Department of CSE(AI&ML), Vasireddy Venkatadri Institute of Technology, Guntur, A.P., India

Assistant Professor, Department of CSE(AI&ML) , Vasireddy Venkatadri Institute of Technology, Guntur, A.P., India

ABSTRACT: The Anonymous Crime Reporting System (ACRS) is an innovative platform designed to facilitate secure and confidential reporting of criminal activities. Leveraging advanced technologies, this system employs Convolutional Neural Networks (CNN) for robust data analysis and Blockchain Ethereum for immutable and transparent record-keeping. The ACRS ensures anonymity for whistleblowers and witnesses, allowing them to report crimes without fear of reprisal. Through CNN algorithms, it processes and analyses reported data, enabling efficient categorization and identification of patterns within reported incidents. The integration of Blockchain Ethereum guarantees data integrity and transparency by creating a tamper-proof ledger of reported crimes. Each report is cryptographically secured, preventing unauthorized access or alteration, thus fostering trust in the system.

KEYWORDS: Anonymous Crime Reporting, CNN, Blockchain Ethereum, Data Analysis, Anonymity, Transparency.

I. INTRODUCTION

In the ever-evolving landscape of technology, safeguarding public safety demands innovative solutions to surmount challenges associated with reporting crimes. Our endeavour, titled the "Anonymous Crime Reporting System," stands at the forefront of this technological evolution as a blockchain-based Anonymous Tip-off system. With a keen focus on harnessing the power of cutting-edge technologies, this web application redefines the dynamics of crime reporting, aiming to overcome barriers that have historically hindered the reporting process.

The "Anonymous Crime Reporting System" addresses a pervasive issue in our society – the underreporting of crimes, particularly in cases involving harassment and abuse. Our web application emerges as a beacon of change, providing a secure and confidential platform that empowers individuals to contribute to community safety without fear of reprisal. Leveraging the accessibility and ease of a web-based interface, our system ensures not only the anonymity of the reporter but also elevates the overall safety and security of our communities.In the following sections, we will delve into the intricacies of this transformative project. The integration of blockchain technology is a key pillar of our approach, ensuring the irrevocable security and privacy of the reported information. Furthermore, the implementation of deep learning techniques adds a layer of sophistication to the system, enabling it to adapt and evolve in the ever-changing landscape of crime patterns.

As we embark on this journey of technological innovation, our aim is to revolutionize the crime reporting process, making it more efficient, trustworthy, and user-centric.

II. LITERATURE SURVEY

The paper by Wang et al. (2021) delves into the fusion of blockchain and machine learning to tackle challenges in secure data sharing. With a spotlight on the 'Proof of Work' mechanism, the authors underscore the significance of bolstering mining success and hash rate elevation to fortify Non-Fungible Tokens (NFTs) against possible breaches. This study advances comprehension of leveraging the collaboration between blockchain and machine learning for robust and secure data sharing in mobile edge intelligence contexts..

Dang et al. (2020) investigate the repercussions of deep fake algorithms on online media content, posing challenges to its credibility. Their study primarily centers on sentiment analysis and the efficacy of deep learning methods in

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203109 |

mitigating obstacles within Natural Language Processing (NLP). Through integrating sentiment and semantic attributes, the authors carry out experiments to assess and contrast the effectiveness of deep learning approaches. Situated within the broader scope of Artificial Intelligence, this research enriches our comprehension of the impact of deep fakes on sentiment analysis and underscores the prospects for enhancement through sophisticated techniques.

The study by Kaur and Saini (2015) offers a thorough examination of text classification algorithms tailored for Indian languages. The burgeoning presence of social media has ushered in a surge in the utilization of diverse languages online, presenting significant hurdles for text classification endeavors. This paper furnishes a meticulous evaluation of numerous text classifiers adept at effectively handling Indian languages. The insights gleaned from this inquiry contribute significantly to augmenting our comprehension of the specific challenges in natural language processing posed by linguistic diversity, particularly within the Indian language landscape.

Furthermore, this literature survey spans a breadth of topics, encompassing the integration of blockchain and machine learning for secure data sharing, the ramifications of deep fake algorithms on sentiment analysis, and the intricacies surrounding text classification for Indian languages. These collective studies serve to propel the advancement of knowledge within their respective spheres and furnish invaluable insights for prospective research and practical applications.

These studies collectively contribute to the advancement of knowledge in their respective domains and provide valuable insights for future research and applications.The comparative analysis of existing methods is presented in below Table 2.1.

Title	Authors Names	Methodology	Limitations	Accuracy	Published Year
Blockchain-based Anonymous Tip-off System	1. Raksha S 2. Samhitha 3. Raipalle 4. Shreya 6. Pranav M S	•The system utilizes blockchain technology for an anonymous crime tip-off mechanism. •Implements a ranking system based on user-provided tips to prioritize reports and maintain anonymity. •Integrates Natural Language Processing (NLP) for auto-categorizing crimes based on keywords in tip descriptions. •Utilizes Machine Learning for ranking events based on parameters such as location, time, and category of crimes.	•The system relies on users having smartphones and internet access. •Potential challenges related to the accuracy of auto-categorizing crimes using NLP. •Dependence on blockchain technology, which may have a learning curve for users unfamiliar with it. •The effectiveness of the system depends on user participation and the willingness of law enforcement to adopt the platform.	The effectiveness of the system depends on user participation and the willingness of law enforcement to adopt the platform. The accuracy of the system will be evaluated based on the successful categorization of crimes, the reliability of tips, and the effectiveness of the ranking system in prioritizing reports.	2022

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203109 |

An Online Crime Reporting System	1.Riya Lohan 2.Mr. Mahesh Singh	•The system is designed to provide a flexible platform for reporting crimes online. •It includes a user-friendly interface for victims/volunteers to lodge FIRs (First Investigation Reports). •The system relies on four reporting forms: a complaint or dispatch reporting form, a crime event report form, follow up investigation report form, and an arrest report form. •Three main functional modules: data capture, report management, and control module, and data utilization module.	•No explicit limitations are mentioned in the provided excerpt. •However, it's advisable to consider potential challenges such as data security, user privacy, and system scalability.	The system aims to improve accuracy by providing a structured and standardized way of reporting crimes, with details like victim information, crime type, and location.	2015
Public Crime Reporting and Monitoring System Model using SDM	1.Priyanka Atmaram Goyar 2.Mayuri Sanjay Patil 3.Shivani Gulab Singh Rajput 4.Dhanashri Gopal Patil	•The paper employs Information Extraction (IE) techniques and principles of the Cognitive Interview. •Information Extraction is likely used to gather relevant details from narratives, and Cognitive Interviewing is a psychological technique aimed at enhancing the recollection of information from witnesses and victims.	•The paper acknowledges various reasons why crimes often go unreported, including emotional factors such as fear and embarrassment, the perception that the crime is insignificant or a personal issue, and challenges in reaching the appropriate authorities.	The system's performance metrics are highlighted, indicating high precision and recall. Specifically, for the Suspect Description Module (SDM), the system achieved a 70% recall and 100% precision.	2019

Table 2.1: Comparative analysis of Existing Methods

III. PROBLEM STATEMENT

Traditional crime reporting systems face critical challenges that impede their effectiveness in ensuring public safety and combating criminal activities. These challenges are rooted in the limitations of existing systems, leading to a pressing need for innovation and improvement. The key problems identified are:

3.1 Lack of Anonymity and Security:

Current crime reporting systems often fail to provide a secure and confidential environment for individuals to report criminal activities. Anonymity is compromised, as fear of retaliation or exposure prevents individuals from reporting crimes, leading to underreporting and hindering law enforcement efforts.

3.2 Inefficient Data Processing and Analysis:

Traditional systems lack advanced mechanisms for processing and analyzing reported data, resulting in delays, inaccuracies, and an inability to identify patterns within incidents. There is a need for sophisticated algorithms to enhance the efficiency of data analysis and categorization, facilitating a more nuanced understanding of reported crimes.

3.3 Vulnerability of Centralized Databases:

Centralized databases are susceptible to tampering, raising concerns about data integrity and transparency. Unauthorized access and modifications pose a significant threat to the reliability of crime-related information stored in centralized systems.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203109 |

3.4 Lack of Trust in Confidentiality:

Mistrust in the confidentiality of existing reporting processes hinders individuals from actively participating in reporting criminal activities. Establishing trust between users, stakeholders, and law enforcement authorities is crucial for the success of any crime reporting system.

3.5 Limited Protection for Witness:

Current systems often lack adequate safeguards to protect the anonymity of witnesses, discouraging them from reporting crimes due to the fear of exposure or retaliation. Whistleblower protection is essential to encourage open and honest reporting without compromising the safety of those involved.

3.6 Inability to Ensure Data Transparency:

The lack of transparency in traditional crime reporting systems raises concerns about the authenticity of reported data. A transparent and verifiable record-keeping system is necessary to build confidence among users, stakeholders, and law enforcement agencies.

3.7 Underutilization of Advanced Technologies:

Many existing systems do not leverage advanced technologies such as Convolutional Neural Networks (CNN) and Blockchain, missing out on opportunities for enhanced data analysis, categorization, and secure record-keeping.

IV. EXISTING SYSTEM

Existing crime reporting systems face challenges in ensuring the anonymity and security of users. Traditional methods often rely on manual reporting, lack advanced data analysis capabilities, and may compromise data integrity. Anonymity concerns and the vulnerability of centralized databases contribute to underreporting and distrust in the system.

4.1 Lack of Anonymity:

Existing systems fail to provide sufficient anonymity, leading to reluctance in reporting crimes.

4.2 Limited Security Measures:

Insufficient security measures make existing systems susceptible to data breaches and unauthorized access.

4.3 Inadequate Data Analysis:

Limited data analysis capabilities hinder efficient categorization and pattern identification in reported incidents.

4.4 Vulnerability to Tampering:

Without proper record-keeping mechanisms, existing systems are vulnerable to data tampering, compromising reliability.

4.5 Lack of Transparency:

The absence of transparent record-keeping methods raises concerns about the accuracy and authenticity of reported data.

V.DATASET

The dataset used for this analysis comprises records of various crimes reported across multiple cities.

Each entry in the dataset includes crucial information such as the date of the incident, the type of crime committed, a brief description of the event, the city where it occurred, and a label indicating the outcome of the crime (successful prosecution or not). By examining this dataset, we aim to uncover insights into the distribution of different crime types, identify patterns across different urban areas, and understand the temporal dynamics of criminal activities. This analysis forms the basis for developing effective law enforcement strategies and informing policy decisions aimed at enhancing public safety.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203109 |

VI. PROPOSED METHODOLOGY

The Anonymous Crime Reporting System(ACRS) addresses these limitations through advanced technologies, prioritizing user anonymity, data integrity, and transparent record-keeping. The integration of CNN, Blockchain Ethereum, and a reward system enhances the system's efficiency, security, and user trust.

This comprehensive approach aims to overcome the deficiencies in the existing crime reporting systems, providing a secure, confidential, and technologically advanced platform for reporting criminal activities.

The methodology employed in the development of the Anonymous Crime Reporting System (ACRS) involves a systematic and collaborative approach, combining advanced technologies to create a secure and efficient crime reporting platform. The key components of the methodology include data analysis using **Convolutional Neural Networks** (CNN), integration of **Blockchain Ethereum** for secure record-keeping, and the implementation of robust security measures.

6.1 False Alarm Detection using CNN:

Utilizing Convolutional Neural Networks (CNN), the system analyzes the descriptions provided in crime reports to distinguish between genuine incidents and false alarms. The CNN model is trained on a dataset of verified crime reports to learn patterns indicative of real criminal activity.

6.2 Multi-Media Upload Functionality:

The system incorporates a versatile multi-media upload functionality, allowing users to submit images, along with their crime reports. This feature enhances the richness of information provided to law enforcement agencies, aiding in more comprehensive investigations and evidentiary support.

6.3 Anonymous Submit Tip-off using Blockchain:

Leveraging the Ethereum blockchain, the system ensures the anonymity and security of tip-offs submitted by users. Each tip-off is encrypted and stored on the blockchain, rendering it immutable and transparent. Smart contracts govern the submission process, ensuring that user identities remain confidential while still enabling authorities to access relevant information for investigation purposes.

6.4 NLP for Description Analysis:

To Natural Language Processing (NLP) is employed to analyse the text description provided by the user. The system auto-categorizes the crime based on keywords, aiding law enforcement in prioritizing reports.

6.5 Exact Time Capturing:

The system incorporates precise time-stamping functionality to capture the exact time when a crime report is submitted. This ensures accurate documentation and tracking of incidents, facilitating timely response and investigation by authorities.

6.6 Performance Evaluation:

The system's performance is continually evaluated based on successful categorization, reliability of tips, and the effectiveness of the ranking system.

VII. SYSTEM ARCHITECTURE

Witness: a person who provide crime information to the police or a person who sees an event, typically a crime or accident, take place. Police are appealing for witnesses to the accident

Police: police extract the information from the witness and generate the questions details storage and police view the report.The entire flow of system is as shown in Fig-7(a).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203109 |

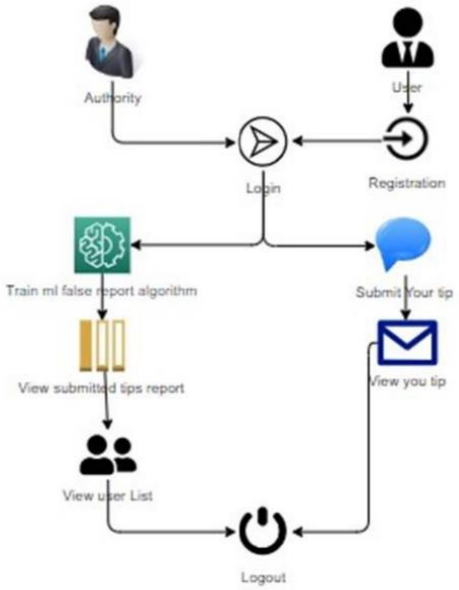


Fig 7(a): System Flow

The proposed Anonymous Crime Reporting System (ACRS) is a revolutionary platform designed to address the shortcomings of traditional crime reporting systems. It leverages state-of-the-art technologies to ensure anonymity, data integrity, and transparency. The key features of the proposed system include advanced data analysis through Convolutional Neural Networks (CNN), Blockchain Ethereum for secure record-keeping, a user-friendly mobile application, and a reward system to encourage user participation.

7.1 Secure and Confidential Reporting:

A user-friendly interface ensures individuals can report crimes anonymously, promoting user safety.

7.2 CNN for Data Analysis:

Advanced algorithms, specifically Convolutional Neural Networks, are employed for efficient data analysis.

7.3 Blockchain Ethereum Integration:

Utilizes Blockchain Ethereum for tamper-proof and transparent record-keeping of reported crimes.

7.4 Witnesses Protection:

Anonymity of witnesses is safeguarded, encouraging reporting without fear of exposure.

7.5 Trust-Building Measures:

Establishes a robust and reliable system to install confidence in users, fostering trust in the reporting process.

7.6 Decentralized Storage:

Implements decentralized storage for effective and cost-efficient crime documentation.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203109 |

VIII. CONCLUSION

As we reflect on the journey of creating the Anonymous Crime Reporting System(ACRS), we recognize its pivotal role in modernizing crime reporting. By incorporating advanced technologies such as Convolutional Neural Networks and Blockchain Ethereum, we've prioritized user anonymity and security, providing a safe space for reporting criminal activities. The user-friendly mobile application and reward system aim to actively engage citizens in community safety. ACRS's advanced data analysis capabilities contribute to a deeper understanding of criminal dynamics, while the transparent and tamper-proof record-keeping system ensures trust. Overall, we envision ACRS as a transformative step toward a future where crime reporting is secure, transparent, and empowers individuals for the greater good of our communities.

X. FUTURE ENHANCEMENT

In future advancements, the Anonymous Crime Reporting System (ACRS) will concentrate on improving user accessibility and augmenting its analytical capacities. This includes the integration of AI-driven chatbots to streamline reporting procedures and enhance user interaction. Furthermore, ACRS endeavors to integrate Natural Language Processing (NLP) for more sophisticated data analysis, enabling the system to decipher unstructured data from reports. Additionally, the incorporation of decentralized identity verification systems will strengthen anonymity while verifying the reliability of submitted information. These upgrades will enhance ACRS's effectiveness, accessibility, and precision in managing reported incidents.

REFERENCES

[1]. Yao Du, Shuxiao Miao, Zitian Tong, Victoria Lemieux & Zehua Wang "**Blockchain-Empowered Mobile Edge Intelligence, Machine Learning and Secure Data Sharing"** - March 2021

[2]. Vishal A. Kharde & S.S. Sonawane, "**Sentiment Analysis of Twitter Data: A Survey of Techniques"** - April 2016

[3]. Jasleen Kaur and Dr. Jatinderkumar R. Saini "**A Study of Text Classification Natural Language Processing Algorithms for Indian Languages"** - – July 2015

[4]. ArcharnaM, Durga S, Saveetha K
"Online Crime Reporting System"

[5]. Riya Lohan and Mr.Mahesh Singth, " **An Online Crime Reporting System**" – Research Paper- June 2015

[6]. B. Holtmann, and Domingo-Swarts, "**Current trends and responses to crime in South Africa. Crime**," Violence and Injury Prevention in South Africa, 2008, pp 105 – 129

[7]. G. Paula, "**Crime-fighting sensors."** Mechanical Engineering Magazine Select Articles, 120 (01), 1998. pp.66-68.

[8]. Kovács, L., Szlávik, Z., Benedek, C., Havasi, L., Petrás, I., Losteiner, D., Utasi, Á., Liscár, A., Czúni, L. and Szirányi, T., "**Video Surveillance Framework for Crime Prevention and Event Indexing**," in ICT4Justice, January 2008.

[9] H. Van Vuuren, "**Small bribes big challenge: Extent and nature of petty corruption SouthAfrica**" South African Crime Quarterly, (9), 2004.

[10] Diva Lal, Adiba Abidin, Naveen Garg, and Vikas Deep. "**Advanced immediate crime reporting to police in India.**" Procedia Computer Science, 85:543–549, 2016.

[11] Tzay-Farn Shih, Chin-Ling Chen, Bo-Yan Syu, andYong-Yuan Deng. **A cloud-based crime reporting system with identity protection**. Symmetry, 11(2):255, 2019.