Crime Alert: Anonymous Crime Reporting System

Nagasivani N[1], Srija Reddy A[2], Naga Sundeep M[3], Vishnu Chaitanya G[4,] Gnanendra K[5]

[1,2,3,4]Department of CSE(AI&ML),Vasireddy Venkatadri Institute of Technology
[1]20BQ1A4239@vvit.net, [2]20BQ1A4204@vvit.net, [3]20BQ1A4232@vvit.net, [4]21BQ5A4202@vvit.net
[5]Assistant Professor,CSE(AI&ML) Department, Vasireddy Venkatadri Institute of Technology
[5]k.gnanendra@gmail.com

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.

1. 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.

2. 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 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
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

3. 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.

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.

4. 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.

5. 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.

6. 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.

7. 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).
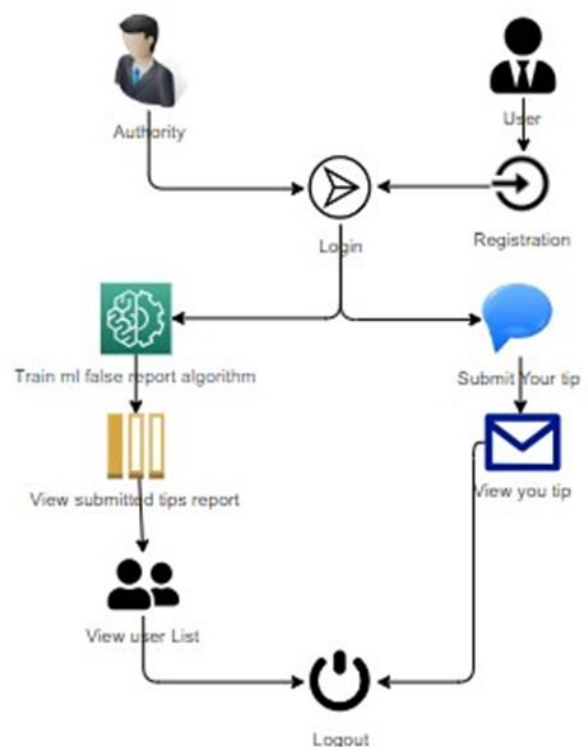

Fig 7(a): System Flow

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.

8. 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.

9. 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.