International Journal of Engineering Research and Science & Technology

DECENTRALIZED CRIME REPORTING SYSTEM USING BLOCKCHAIN

GUIDE

[1]Name : Mrs. DR. B. PHIJIK MTech. PhD

Assistant Professor

[2]B. AMULYA

[3]B. VYSHNAVI

[4]B. MANISHA

[5]D. VYSHNAVI

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
VIGNAN'S INSTITUTE OF MANAGEMENT AND TECHNOLOGY FOR WOMEN
(An Autonomous Institution)
(Affiliated to Jawaharlal Nehru Technological University Hyderabad, Accredited by NBA,NAAC with A+)
Kondapur(Village), Ghatkesar (Mandal), Medchal (Dist.)
Telangana-501301

(2025-2026)

ABSTRACT

This report presents the development of a crime reporting and analysis system that leverages blockchain technology to facilitate secure and anonymous crime reporting. The platform features two distinct interfaces: one for users to submit reports and receive updates on their status, and another for authorities to access and analyse the reports submitted by the public. Utilizing the immutability and transparency features of blockchain, the system ensures that reports are securely stored and tamper-proof, encouraging greater public participation in crime reporting without fear of retaliation. each user is assigned a unique, non-identifying username, allowing for anonymity while still maintaining an organized reporting system. Each user is assigned a unique, non-identifying username to maintain anonymity while enabling organized report management. Smart contracts are employed to automate report submission, generate

case IDs, and update case statuses, ensuring efficiency and minimizing manual intervention.

Keywords

Blockchain, Decentralized Systems, Crime Reporting, Smart Contracts, Machine Learning, Fake Report Detection, Data Immutability, Ethereum, Django Framework, SHA-256 Hashing, Web3 Integration, Transparency, Cybersecurity, Data Integrity, Naïve Bayes, Logistic Regression

I. INTRODUCTION

The advancement of digital technologies has significantly transformed the way public services are delivered, including crime reporting systems. Traditional crime reporting methods are primarily centralized, where data is controlled and managed by a single authority such as law enforcement agencies. Although these systems provide basic functionality, they suffer from several limitations, including lack of transparency, vulnerability to data tampering, delayed processing, and limited user trust. Citizens often hesitate to report crimes due to fear of exposure, lack of anonymity, and uncertainty regarding the status of their complaints. These challenges highlight the need for a more secure, transparent, and user-centric approach to crime reporting.

To overcome these limitations, the proposed system introduces a **Decentralized Crime Reporting System using Blockchain**, which leverages modern technologies to ensure data integrity, transparency, and security. Blockchain technology plays a crucial role in this system by providing an immutable and tamper-proof ledger where crime report data is securely recorded. Once stored, the information cannot be altered or deleted, ensuring reliability and trustworthiness. The decentralized nature of blockchain eliminates the dependency on a single authority, thereby reducing the risk of system failure and unauthorized data manipulation.

In addition to blockchain, the system integrates **machine learning techniques** to enhance the efficiency and accuracy of crime reporting. A classification model is used to analyze submitted reports and detect fake or spam entries. By applying text preprocessing methods and algorithms such as TF-IDF, Logistic Regression, and Naïve Bayes, the system ensures that only valid reports are processed further. This reduces manual workload on authorities and improves the overall quality of the data being handled.

The system is implemented as a web-based application using the Django framework, providing an interactive and user-friendly interface for both citizens and law enforcement authorities. Users can register, submit reports, and track the progress of their complaints, while authorities can review, verify, and update report statuses efficiently. To maintain user privacy, the system assigns non-identifying usernames, enabling anonymous reporting without compromising accountability.

II. LITERATURE REVIEW

The integration of blockchain technology into public service systems has gained significant attention in recent years, particularly in domains requiring high levels of security, transparency, and trust. Early research focused on utilizing blockchain for secure data storage in crime reporting systems. Studies such as those by Sharma and Gupta (2020) proposed blockchain-based frameworks to ensure that crime reports remain immutable and tamper-proof. Their work highlighted the ability of distributed ledgers to prevent unauthorized modifications and improve data integrity. However, these systems primarily focused on secure storage and lacked intelligent mechanisms to validate the authenticity of submitted reports.

Subsequent research explored the application of blockchain in broader e-governance systems. Singh and Kumar (2021) emphasized the role of blockchain in enabling anonymous reporting and maintaining permanent records. Their work demonstrated that decentralization enhances citizen trust and accountability. However, these systems were not specifically tailored for crime reporting and often lacked scalability and real-time processing capabilities. Similarly, Patel and Reddy (2021) introduced a blockchain-based public safety reporting platform that enabled real-time monitoring of complaints. While their approach improved transparency and system responsiveness, it did not incorporate advanced techniques for detecting fake or misleading reports, which remains a critical challenge in open reporting platforms.

With the advancement of intelligent systems, researchers began integrating artificial intelligence with blockchain. Wang and Lee (2023) proposed an AI-integrated blockchain platform for crime management, where machine learning algorithms were used to validate reports before storing them on the blockchain. This approach significantly improved system efficiency and reduced manual workload. However, the implementation complexity and high computational requirements posed

challenges for large-scale adoption. In a similar direction, Mehta and Verma (2023) developed a decentralized crime reporting system that ensured transparency and accountability but lacked strong anonymity features and faced scalability issues due to blockchain transaction costs.

Recent studies have focused on enhancing privacy and scalability. Zhou et al. (2024) introduced a zero-knowledge proof-based system to enable anonymous yet verifiable crime reporting. This approach provided strong privacy guarantees but increased computational overhead and system complexity. Arora and Singh (2025) proposed a Layer-2 blockchain solution to address scalability issues by reducing transaction costs and improving throughput. While this approach enhanced performance, it introduced additional technical complexity and did not fully address privacy concerns.

Despite these advancements, existing systems still exhibit several limitations, including lack of efficient fake report detection, high implementation complexity, scalability constraints, and insufficient user anonymity. Moreover, many solutions focus either on blockchain security or machine learning intelligence, but not both in a unified framework.

To address these gaps, the proposed system combines blockchain technology with machine learning techniques to create a secure, transparent, and intelligent crime reporting platform. By integrating fake report detection using classification algorithms along with tamper-proof blockchain storage, the system enhances both data reliability and operational efficiency. Additionally, the use of user anonymity and real-time tracking features further strengthens user trust and system usability, making it a comprehensive improvement over existing approaches.

III. METHODOLOGY

1. System Workflow Overview

The methodology begins with user interaction through a web-based interface. Users register and log in to the system, after which they can submit crime reports containing details such as title, description, location, and optional media. The submitted data flows through multiple stages including validation, machine learning analysis, hashing, blockchain storage, and database recording.

2. Data Collection and User Interaction

The system provides a user-friendly interface developed using HTML, CSS, and JavaScript. Users can:

- Register with secure credentials
- Log in to the platform
- Submit crime reports
- Track report status

3. Text Preprocessing

Before applying machine learning algorithms, the textual content of crime reports undergoes preprocessing to improve data quality. This includes:

- Converting text to lowercase
- Removing punctuation and special characters
- Eliminating stop words (e.g., "the", "is")
- Tokenization (splitting text into words)

4. Feature Extraction using TF-IDF

The processed text is converted into numerical format using **Term Frequency–Inverse Document Frequency (TF-IDF)**. This technique assigns weights to words based on their importance in the document relative to the dataset. The result is a feature vector that represents the textual data in a form suitable for machine learning models.

5. Machine Learning-Based Classification

The system employs classification algorithms such as **Logistic Regression** and **Naïve Bayes** to determine whether a report is genuine or fake.

- If the report is classified as **fake**, it is rejected immediately.
- If classified as **real**, it proceeds to the next stage.

6. Cryptographic Hash Generation (SHA-256)

For valid reports, a cryptographic hash is generated using the **SHA-256 algorithm**.

- The hash acts as a unique digital fingerprint of the report
- Any modification in the report results in a completely different hash

7. Blockchain Integration

The generated hash is stored on the blockchain using **Ethereum smart contracts**. The system uses:

- **Ganache** as a local blockchain environment
- **Solidity** for writing smart contracts
- **Web3.py** for interaction between Django and blockchain

8. Database Storage

While the blockchain stores only the hash and metadata, the complete report details

International Journal of Engineering Research and Science & Technology

are stored in a **SQLite database**. This approach:

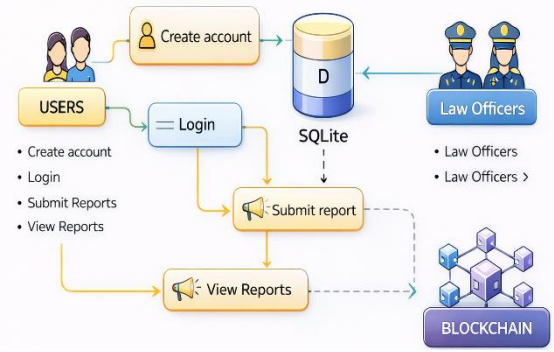
- Maintains efficiency and scalability
- Protects sensitive user information
- Enables fast retrieval and updates

9. Authority Module

Authorized personnel (law enforcement officers) can:

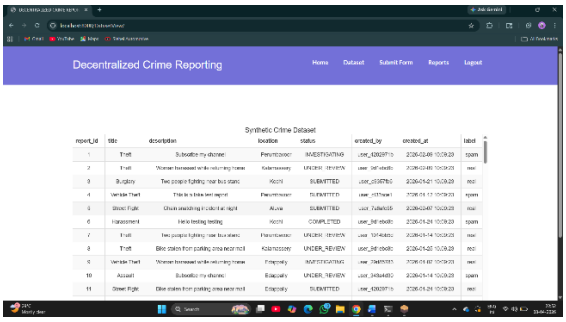
- Access submitted reports
- Verify and analyze data
- Update report status (e.g., pending, verified, resolved)

IV. SYSTEM ARCHITECTURE



V. RESULTS & DISCUSSION

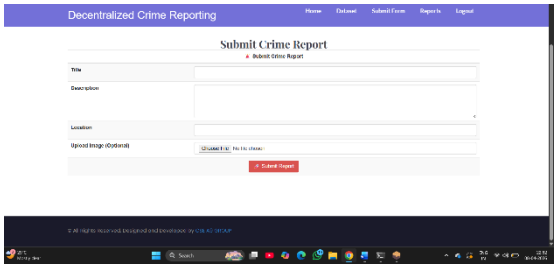
The implementation of the decentralized crime reporting system demonstrates that the integration of blockchain technology and machine learning significantly enhances the overall efficiency, security, and reliability of crime reporting processes . The system was thoroughly tested across multiple modules, including report submission, machine learning validation, blockchain storage, and database management. The results indicate that all components function cohesively, ensuring a smooth and accurate workflow from user input to final data storage. The web-based interface successfully enables users to submit reports and track their status, while authorities can efficiently manage and update case information.

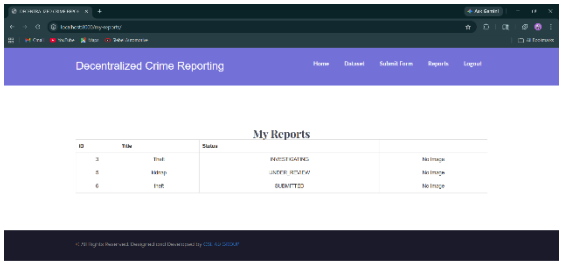


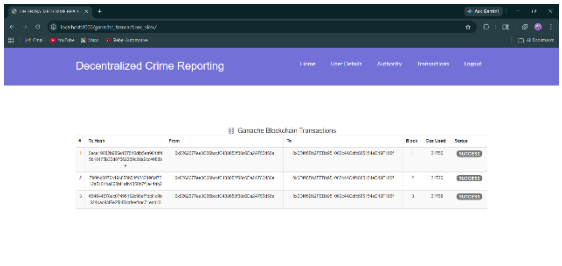
The machine learning module plays a critical role in improving system performance by accurately classifying reports as genuine or fake. With an achieved accuracy of approximately 95%, the model effectively filters out spam or misleading entries before they are processed further. This significantly reduces the burden on law enforcement authorities and ensures that only relevant

International Journal of Engineering Research and Science & Technology

and valid reports are considered. The preprocessing techniques and feature extraction methods contribute to the robustness of the model, enabling it to handle textual data efficiently.







From a security perspective, the use of the SHA-256 hashing algorithm ensures that each crime report is converted into a unique digital fingerprint. This hash is then stored on the blockchain, guaranteeing data immutability and preventing any unauthorized modifications. The blockchain integration, implemented using Ethereum and tested through Ganache, successfully records each transaction with a unique identifier. This provides a transparent and verifiable record of all submitted reports, enhancing trust and accountability within the system.

Performance evaluation shows that the system is capable of handling multiple report submissions with minimal delay. The average response time of approximately 1.5 seconds per report indicates that the system is efficient and responsive. Even under concurrent user activity, the system maintains stability without data loss or processing errors. The database module also performs reliably by storing complete report details and transaction IDs, ensuring proper data management and easy retrieval.

Despite these positive outcomes, certain limitations were observed during testing. The current implementation relies on a local blockchain environment, which may differ from real-world blockchain networks in terms of scalability and transaction costs. Additionally, the effectiveness of the machine learning model depends on the quality and diversity of the training dataset. These limitations suggest opportunities for future improvements, such as deploying the system on a live blockchain network and enhancing the model with advanced deep learning techniques.

VI. CONCLUSION

The Decentralized Crime Reporting System using Blockchain presents an effective and modern solution to the limitations of traditional crime reporting mechanisms. By integrating blockchain technology with machine learning, the system successfully ensures security, transparency, and reliability in handling crime-related data . The use of a decentralized architecture eliminates the risks associated with centralized systems, such as data tampering, single points of failure, and lack of accountability.

The implementation of machine learning techniques for fake report detection significantly improves the quality of submitted data by filtering out spam or invalid entries. This reduces the workload on law enforcement authorities and enhances the overall efficiency of the system. At the same time, the use of cryptographic hashing (SHA-256) and blockchain storage ensures that once a report is recorded, it remains immutable and verifiable, thereby strengthening data integrity and trust.

The system also emphasizes user privacy by allowing anonymous reporting through non-identifying usernames, encouraging greater public participation. Additionally, features such as real-time status tracking and automated processes using smart contracts contribute to transparency and faster response handling. The successful testing of the system demonstrates its robustness, with accurate classification, efficient performance, and seamless integration of all components.

REFERENCES

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
2. G. Wood, “Ethereum: A Secure Decentralized Generalized Transaction Ledger,” Ethereum Yellow Paper, 2014.
3. V. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum White Paper, 2014.
4. N. Szabo, “Smart Contracts: Building Blocks for Digital Markets,” 1996.
5. T. M. Mitchell, *Machine Learning*, McGraw-Hill Education, 1997.
6. I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.
7. F. Pedregosa et al., “Scikit-learn: Machine Learning in Python,” *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.
8. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain

Technology: Beyond Bitcoin," *Applied Innovation Review*, 2016.

9. A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016.
10. J. Dean and S. Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters," *Communications of the ACM*, 2008.