WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

AI-Driven Cyber Crime Reporting and Classification System Using Logistic Regression

Mr Sandesh R*[1], Anusha R*[2], Chandana K*[3], Jeevitha R*[4], Lochana A R *[5]

[*1] Assistant Professor, CSE, ATME College of Engineering, Mysuru, Karnataka, India
[*2,3,4,5] Students, CSE, ATME College of Engineering, Mysuru, Karnataka, India

ABSTRACT

The internet has given rise to a very high number of cybercrimes including phishing, financial fraud, identity theft, impersonation, and online harassment due to the rapid development of internet platforms. To overcome the issue of false and slow reporting, the current work suggests a single AI-driven Cybercrime Reporting and Management System to be used by combining speech-to-text input, the TF-IDF-based NLP, and the Scikit-learn-based Logistic Regression. The 10,800 labeled complaints, broken down into 88 subtypes, which were reported in 10 broad categories of crime, were trained on and gave a subtype accuracy of 85.97 with an almost perfect mapping to 10 major categories. The system promotes the upload of image and video evidence, automated safety tips, chatbot support, and safe generation of PDF reports with the help of Flask, MySQL, and ReportLab. The outcomes of the experiments show that easier access, decreased time of reporting, and increased accuracy of such submissions and completeness of submissions of cybercrime complaints are achieved.

Keywords- Cybercrime, Logistic Regression, TF-IDF, NLP, Scikit-Learn, Speech Recognition, Web Speech API, Flask, Machine Learning.

1.INTRODUCTION

The number of cybercrimes is growing across every part of the globe, following the popularization of online communication, electronic transactions, and social media. Phishing, identity theft, financial fraud, impersonation, and online harassment are some of the crimes that have been advanced and thus hard to identify and report. The victims are not always ready to report due to poor technical knowledge about what has happened, problems in explaining what has happened, and a lack of understanding of the types of crime. Current reporting portals lack speech based reporting, intelligent classification, multimedia evidence submission in structured format, and thus end up incomplete and delayed investigations. To address these issues, the proposed paper introduces an AI-based system of cybercrime reporting and management based on Natural language processing (NLP), machine learning, and speech recognition. The system allows entering complaints using the speech-to-text interface, classifying crimes automatically with the help of the TF-IDF and Logistic Regression trained on 10,800 samples, uploading multimedia evidence, chatbot support, safety recommendations, and automatic generation of PDF reports. The model will have 85.97 percent accuracy at subcategory level and 100 percent accuracy at main crime type, which is more useful and efficient in investigation.

2.PROBLEM STATEMENT

Some of the most widespread cybercrimes include phishing, online frauds, cyber bullying, identity theft and impersonation over the internet which are becoming hard to report on properly and in time. The vast majority of the victims do not have enough digital knowledge and struggle to determine what specific type of crime they have encountered. In other instances, the users also find it difficult to articulate the details of the incident. Current cybercriminal reporting websites lack comprehensive instructions and do not give an opportunity to enter a complaint by speaking. Lack of multimedia evidence upload also makes reported cases less complete. Even though machine learning models can be useful in categorizing cybercrime trends, these data are not often presented in secure and accessible public systems. This has led to delays in reporting, misclassification and incomplete documentation. In order to overcome such drawbacks, this project will implement a full-stack AI-based cybercrime reporting/management system, which will enhance the accessibility, accuracy, and reliability of complaint reporting.

3.LITERATURE REVIEW

Mantoro et al. [1] were concerned with automated categorization of unstructured accounts of crime based on text mining. The system applied a strict pre-processing pipeline that involved tokenization, stop-word removal and noise filtering of the short, noisy text descriptions. The authors applied the Logistic Regression algorithm as the main classifier in the task. According to the research, the accuracy of this method was high at 90 percent, which was due to

the effectiveness of this algorithm in dealing with high-dimensional text characteristics, as well as the isolation of pertinent keywords of crime in noisy unstructured data without the need to overfit.

Ahsan et. al. [2] introduced Data Mining and Machine Learning (DM-ML) framework to automate the process of analyzing the global cyber incident report. To be able to process the textual descriptions, the system used the Term Frequency Inverse Document Frequency (TF-IDF) to turn the text into number. This approach enabled the model to in an intelligent manner weigh up important terms (such as malware) and screen out typical noise. A Logistic Regression was used in the study to categorize these TF-IDF vectors. The findings proved the hypothesis that this particular TF-IDF feature extraction and Logistic Regression combination offered an effective solution to the problem of classifying the dense crime stories by converting the raw text into fine grain numerical elements.

Hasan et al. [3] were able to solve the problem of online harassment by creating an automated detecting system. The scholars used a pre-processing pipeline, which included tokenization and stop-word elimination to make informal social media text clean. The classification of comments into Bullying and Non-Bullying was carried out using the system of Logistic Regression. This study had a 95% accuracy, which can be attributed to the fact that the model placed a high weight on the unique aggressive keywords (particular slurs) that can effectively distinguish abusive content and harmless text.

Kumar et al. [4] created a machine learning model to automate credit card and online transactions fraud detection. To deal with the limited number of cases of fraud in the data, the system used a data balancing method of the SMOTE (Synthetic Minority Over-sampling Technique) so that the data is balanced. The authors used the Logistic Regression as a binary classifier. The system was able to conduct an accurate determination of about 97-99% and effectively detect the fraud patterns that were linear like transaction amounts that were unusual. The paper has pointed out that the speed and explainability of the model make it suitable in financial security systems that are required in real time.

4. METHODOLOGY

The proposed AI-Based Cybercrime Reporting and Management System is designed in the framework of a multilayered architecture that is oriented on a user-friendly approach, automation, precise machine learning-based classification, and safe management of sensitive complaint data. The system combines a Scikit-Learn machine learning framework which is a Logistic Regression model, a speech-enabled interface, multimedia evidence upload, and a full-stack web platform. Fig. 1 shows the system functional workflow.

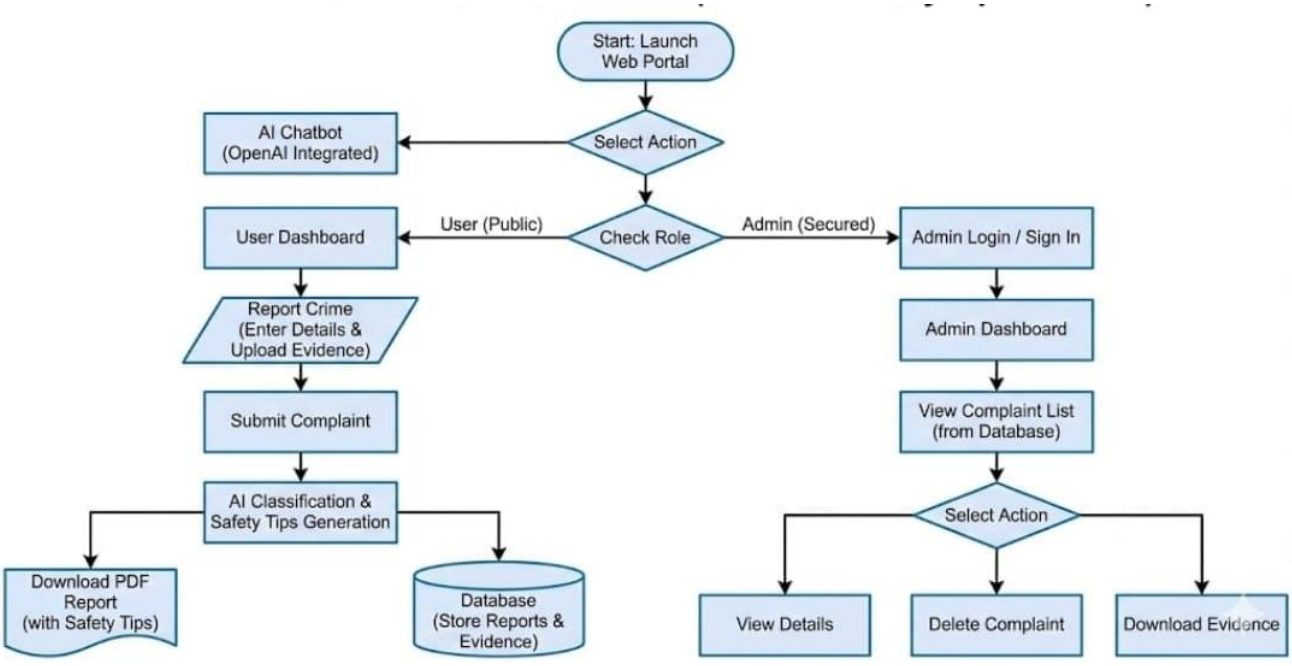

Figure 1: system functional workflow.

4.1 Requirements

The system requirements are divided into functional and non-functional ones.

4.1.1 Functional Requirements

Registration of users and submission of complaints- The system should enable users to use a text or voice to type personal details, details of incidents, and narration.Speech-to-Text Enabled Input- The interface should also allow real-time speech narration with Web Speech API and should directly transform it into a text.Evidence Upload- The users need to be in a position to post multimedia evidence including pictures, screen shots and video files.

AI Classification- The system should categorize the description of the complaint in 88 subtypes and must be mapped to one of the 9 broad categories of cybercrime. PDF Generation- The users can be allowed to download a generated report summarizing the incident, classification, and safety tips.Admin Review- Administrators should be allowed to interpret, edit, delete and download reports.

4.1.2 Non Functional Requirements

Security- Sensitive data and evidence of complaints should be maintained in a secure manner and strict routing should be maintained and safe file storage ensured. Usability- The user interface should be responsive, accessible and intuitive to non technical victims. Reliability- The system is to be strong in different network and load conditions .Performance- The classification of crime cannot be delayed on the server because it has to be interactive.

4.2 System Architecture

As indicated in the three tier architecture your system architecture will be described as:

Frontend: This layer enables the visualization of the system. The frontend is a development of HTML, CSS and JavaScript. Users provide information, narrate an incident with speech and purchase digital evidence. The interface interacts with the backend through the RESTful POSTs.

Application Layer (Backend): Python Flask is used to validate input, perform ML inference, create PDFs and file manipulation. Load Scikit -Learn TF-IDF vectorizer and subtype by Logistic Regression classifier. Prognosticate sub type into central type.Formulates individual safety recommendations. Handles the multimedia files safely.

Data Storage: The MySQL database keeps records of complaints, user information, trail of evidence and classification outcome. The PDF reports get stored into a specific route

4.3 Tools and Technologies

Backend: Python, Flask-REST API and business Logic, TF-IDF Vectorixxzation and Multinomial Logistic Regression, ReportLab for PDF Generation

Database: MySQL for Database Management.

Frontened:HTML5,CSS3,JavaScript for User interface

4.4 Challenges and Solutions

Class Imbalance in Subtype Dataset: The study shows that Imbalance in Classes occurs in Subtype Dataset. Other subtypes were smaller and, therefore, predictive performance decreased.Solution: Evened out the data in various CSVs and stratified the sample so that training occurred fairly.

Assuring Accuracy Mapping of Type of Crime: Misclassification on the top levels is subtype. Solution: Applied deterministic mapping so that it was guaranteed to be 100 percent accurate at the major type of crime level.

5.RESULT AND DISCUSSION

The suggested AI-based model of cybercrime classification was trained on the data of 10,800 complaints descriptions, grouped into 10 major types of crimes and 88 subtypes. The standard machine learning performance measures were used to test the model. Here, the results of the experiment are provided and the effectivity of the system to classify fine-grained subtypes of cybercrime is examined.

The model of subtype classification was accurate with the 85.97 percentage that indicates the usefulness of TF-IDF vectorization-based on Multinomial Logistic Regression to classify text-based cybercrimes. Table 2 is a summary of the overall performance measures.

Metric	Score
Accuracy	85.97%
Precision	0.89
Recall (Weighted Avg)	0.87
F1-Score (Weighted Avg)	0.86

Table 2:Overall Performance measure

6.FUTURE RESEARCH AND DEVELOPMENT

The system can be further developed as future work in order to use deep learning-based language models, like BERT or Bi-LSTM networks, to enhance the accuracy of classification in complex categories of harassment and crime involving emotional expressions. Other improvements can be real-time

image and video forensic analysis, cross-platform social media incident detection, multilingual complaint support, and automatic prioritization of cases based on the level of threat. Such extensions will enhance the intelligence and scalability of AI-based cybercrime reporting systems and give them a real-world impact.

7.CONCLUSION

The offered system is a fully AI-driven cybercrime reporting and managing system that unites TF-IDF-based natural language processing with a Multinomial Logistic Regression classifier as a way of automatizing the process of cybercrime detection. The model was trained over 10,800 real-world cybercrime complaints of 88 subtypes and 10 major crime categories with a subtype classification accuracy of 85.97% and a hierarchical mapping of crime-types with near-perfect accuracy. These findings substantiate the fact that classical machine learning coupled with the appropriate NLP feature extraction is accurate and appropriate in real-time reporting of cybercrimes. Other than the model performance, the system provides an entire end-to-end digital reporting platform with speech-to-text complaint entry, upload image and video evidence, automatic safety tips, chatbot-assisted support, and secure PDF report generation, and an administrative dashboard to monitor the case. This unified framework enhances accessibility, the precision of reports, and administrative efficiency meaning the system is viable to be deployed in law enforcement agencies, educational institutions, and online public digital governance platforms.

8.REFERENCES

[1] T. Mantoro, W. A. Wibowo, and H. D. Surjono, "Crime Rate Detection Based on Text Mining on Social Media Using Logistic Regression Algorithm," in 2021 IEEE 7th International Conference on Computing, Engineering and Design (ICCED), Sukabumi, Indonesia, 2021, pp. 1-6.

[2] M. Ahsan, M. A. Khan, M. A. Al Ghamdi, and S. H. Almotiri, "Classification and Prediction of Significant Cyber Incidents (SCI) Using Data Mining and Machine Learning," IEEE Access, vol. 11, pp. 94486-94496, 2023.

[3] M. Hasan, M. A. Alauthman, S. Yonbawi, and A. Almomani, "Cyberbullying Detection and Recognition with Type Determination Based on Machine Learning," Computers, Materials & Continua, vol. 75, no. 3, pp. 5310-5325, 2023.

[4] A. Kumar, S. Sharma, and R. Gupta, "Financial Fraud Detection using Machine Learning and Deep Learning Models," in 2025 International Conference on Computing and Communication Systems (ICCCS), IEEE, 2025, pp. 1-6

[5] M. Singh, H. Mall, R. Choudhary, A. Khandelwal, and S. Verma, "Efficient Chatbot for Complaint Registration," i-manager's Journal on Software Engineering, vol. 16, no. 4, pp. 1–8, 2022.

[6] M. Ahsan, M. A. Khan, M. A. Al Ghamdi, and S. H. Almotiri, "Computational System to Classify Cyber Crime Offenses using Machine Learning," Sustainability, vol. 12, no. 10, Art. no. 4087, 2020.

[7] F. Silva, A. Antunes, and B. H. Wixom, "The Implementation of Public Chatbots to Raise Awareness of Computer Crime," International Journal of Human–Computer Interaction, vol. 40, no. 1, pp. 1–18, 2024.

[8] A. Mishra and A. Soni, "SMSDect: A Prediction Model for Smishing Attack Detection Using Machine Learning and Text Analysis," in 2023 International Conference on Data Science and Network Security (ICDSNS), IEEE, 2023, pp. 1–6.