International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

An automated spam detection and location-based monitoring system

Moksha Kothari [1,*] and Prakash Bethapudi [2]

[1] *Department of Information Technology, GMR Institute of Technology, Rajam, Srikakulam, India.*
[2] *Department of Information Technology& Computer Applications, Andhra University, Visakhapatnam, India.*

International Journal of Science and Research Archive, 2024, 13(02), 1712–1722

Publication history: Received on 13 October 2024; revised on 22 November 2024; accepted on 25 November 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.13.2.2272

Abstract

Spam is often considered as the most troublesome aspect in digital era with security and privacy concern. It is essential to develop effective solutions for spam issues. This project Automated spam detection and location-based monitoring system, provides a new detection system of spam attack in calls, messages and emails. It also provides location-based monitoring of these attacks. It relies on machine learning algorithms trained with updated datasets to accurately classify calls, messages and emails into spam. Through various sophisticated natural language processing techniques, it detects message and email spam content and patterns in call logs for identifying known spam numbers. It provides an interface through which user can enter a phone number or email address to detect spam. As soon as it detects a spam, the details are displayed with timestamp, and an alert is sent to user through email or SMS. The system also integrates location-based tracking to determine the geographic source of spam details. Leveraging geolocation data gathered from calls and account information, this feature aims for fraud prevention and situational awareness. Map visualization keep the insights actionable and transparent. The spam and location together form a single solution for real-time data processing / spam detection /location tracking that can be both seen as an application on its own or integrated into other platforms, making a very powerful weapon in fighting digital fraud while enhancing secured communication. This project provides practical applications for all users to facilitate a safer communication environment with greater accountability.

Keywords: Spam Detection; Location Monitoring; Call Logs Analysis; Email Spam Filtering; Geolocation Tracking; Real-Time Detection

1. Introduction

In the digital age, fraudulent transactions pose a significant threat to individuals and businesses alike. With increasing reliance on mobile communication, tracing suspicious activities through recent call logs, SMS, and URLs has become a vital strategy for identifying and preventing fraud. This system is designed to leverage user inputs such as mobile numbers and account numbers to trace potential fraudsters by classifying spam calls and messages. Upon detecting spam within the last 24 hours, the system will further track and display the location of the fraudster on a map interface.

By analyzing account data in real-time, it can quickly flag suspicious patterns in transaction behavior, like unusually large withdrawals or transfers that deviate from a user's typical banking habits. Additionally, spam link analysis, often overlooked, plays a crucial role in identifying phishing attempts and other deceptive methods that cybercriminals use to gain unauthorized access to sensitive account information. By integrating multiple data points—geographical, transactional, and external phishing links—this holistic approach offers a comprehensive defense mechanism that strengthens the resilience of online banking platforms in today's increasingly digital economy.

* Corresponding author: Moksha Kothari

2. Literature survey

2.1. Comprehensive Review of Cybercrime Detection Techniques

In article [1], the authors, Wadha, A. et. al, came up with Comprehensive review of cybercrime detection techniques. Proceedings of IEEE Access, Special Section on Emerging Approaches to Cyber Security. The authors in this paper had explained different types of cyber-crimes in detail and also explained how such activities take place. Types of cyber-crimes discussed in this paper are:

- Cyber Terrorism
- Cyber Warfare
- Cyber Espionage
- Child Pornography
- Phishing
- SQL Injection Attack.

Cyber-crime detection techniques used here are: Statistical method, Machine learning method and Data mining method. By the use of machine learning and data mining methods, cybercrime detection techniques is accurate and fast. However, many existing approaches are somewhat narrow in their scope and focus on individual types of cybercrimes and dangers — missing potentially larger threats. The most widely used technologies includes statistics, neural networks, fuzzy logic classifiers and WEKA which supports a variety of algorithms for text classification in cyberbullying detection. Some of the most popular algorithms that one can use are decision trees, SVM, naïve Bayes and K-means clustering but these suffer from noise in training data. There is much requirement of more complete datasets and a combination of different detection methods in future studies to be able to stay one step ahead of continuously evolving cyber-attacks.

2.2. Banking Information Resource Cybersecurity System Modeling

In article [2], the author Shulha, Olha, et al worked on the topic . "Banking information resource cybersecurity system modeling. " Journal of Open Innovation: Technology, Market, and Complexity (2022)Banking systems are subject to constant cyber threats, therefore the development of cognitive models for assessing the level of cybersecurity in a banking system is crucial The authors: Olha Shulha, Iryna Yanenkova, Mykhailo Kuzub, Iskandar Muda and Viktor Nazarenko Using fuzzy cognitive maps to model the state of cybersecurity Their work highlights the importance of information protection from external and internal dangers. Their approach provides benefits such as predicting state of cyberspace and deployment of protective measures to ensure safety aspects which enabled better management of security. A drawback however is that current methods may fail to consider relevant vulnerabilities and the way they affect the system. Those algorithms are based on fuzzy set theory for quantify risk, which is a more delicate analysis of risks and threatens. Cognitive modeling and fuzzy logic are technologies applied in their research that can analyze the complex relationships between different risk factors. The paper did not state any accuracy measures, although it is suggested that the cognitive models will provide robust systems to evaluate and enhance the cybersecurity protocols of banks, resulting in an elevated security atmosphere. Algorithms such as fuzzy production models and causal relationship models help assess risks by analyzing connections between risk factors and impacts. Future research could focus on developing integrated risk management frameworks and expanding cybersecurity measures to address evolving threats.

2.3. Cybercrime Unmasked: Investigating Cases and Digital Evidence

In article [3], the author is Azam, Hamza, et al. whose work is about "Cybercrime Unmasked: Investigating cases and digital evidence. " International Journal of Emerging Multi-disciplinaries Computer Science & Artificial Intelligence (2023). The paper explores the rise of cybercrime, emphasizing the importance of digital forensics and evidence in legal investigations. It outlines the five phases of digital forensics and discusses various types of cybercrime, including cyberbullying, data theft, ransomware, phishing, and identity theft. This paper provides an in-depth review of digital forensics coupled with a closeup of the five key elements: acquisition, preservation, analysis, reconstruction and presentation of digital evidence. The paper describes some examples of cyber basics, prison cell crime device types incorrectly known as offenders and the manner within which such crimes are committed inclusive of cyber bullying, cybersecurity issues, information theft attack cases to name but a few along with example cases for better understanding. Business Stakeholders Paper Digital Forensics Cyber Crime The evidence analysis tools used are forensic tools including FTK Imager; EnCase; Autopsy. For collecting, preserving, and analyzing digital evidence, forensic tools play a vital part Technologies such as MD5 or SHA-1 are used to create hashes for the evidence being

collected; thus ensuring that it is intact and not altered throughout the context. It also includes best practice for handling pieces of evidence that can raise the bar on investigations: How to investigate a better way so that they become good at work. Investigations are complicated because of the rapid evolution of technology in the digital forensics field. It is proposed that improving forensic processes, like having a chain of custody and making use of higher technology, would translate into better investigations done to find the perpetrator.

2.4. Financial Fraud and Credit Risk: Illicit Practices and Their Impact on Banking Stability

In article [4], the authors are Afjal, Mohd, Aidin Salamzadeh, and Léo-Paul Dana. "Financial fraud and credit risk: Illicit practices and their impact on banking stability. " Journal of Risk and Financial Management 16 (2023). The literature on cybercrime, particularly focusing on scams, highlights both advantages and disadvantages of current methodologies in identifying and classifying scam types. One significant advantage is the reduction of over 35 ambiguous scam categories into 7 distinct genres through hierarchical clustering and discriminant function analysis, which enhances the clarity and effectiveness of scam identification. This classification framework not only aids law enforcement agencies in tracking and monitoring cybercrimes but also provides a comprehensive understanding of the business processes adopted by scammers. A disadvantage is the overclassification of scams in existing literature, which can lead to confusion and misidentification of scam types. The research also emphasizes the importance of static features in identifying scams, with only 68 out of 82 features required to achieve a 95% accuracy level, indicating a potential for streamlining the identification process. In terms of datasets, the study analyzed over 250 scam cases sourced from 14 different reporting agencies, providing a rich foundation for understanding scam processes. The technologies employed include statistical analysis methods such as cluster and discriminant function analysis, which are crucial for identifying patterns within the data. Future research could explore the integration of routine activity theory and lifestyle-exposure theory to further enhance the understanding of cybercrime victimization and target identification. Additionally, there is a need for ongoing research into the evolving nature of scams and the technological advancements that scammers may exploit, ensuring that classification frameworks remain relevant and effective in combating cybercrime.

2.5. The Seven Scam Types: Mapping the Terrain of Cybercrime

In article [5], the authors Stabek, Amber, Paul Watters, and Robert Layton. "The seven scam types: mapping the terrain of cybercrime. " 2010 Second Cybercrime and Trustworthy Computing Workshop. IEEE. The literature survey of the given paper focuses on the interconnected relationship between financial fraud, credit risk, and banking stability. The study employs a comprehensive bibliometric analysis to identify key trends, patterns, and research networks in the field. The primary data source for this research is the Scopus database, which provided a total of 2790 documents spanning from 1990 to 2023. This dataset includes various document types such as articles (1853), books (504), book chapters (218), conference papers (38), and reviews (177). The bibliometric analysis offers a holistic overview of the current research landscape, revealing significant patterns and trends that inform future research directions. The use of advanced tools like Biblioshiny and VOSviewer allows for a detailed visualization of research networks and collaboration trends among authors, enhancing the understanding of the field. The study may be limited by the scope of the Scopus database, which, while extensive, may not encompass all relevant literature in the field of financial fraud and credit risk. The reliance on bibliometric methods may overlook qualitative insights that could be gained from in-depth case studies or interviews. The research utilizes bibliometric analysis techniques, including keyword frequency evaluation, bibliographic coupling, and co-citation analysis. The study highlights the need for future research to adopt a more integrative approach when examining financial fraud and credit risk, considering their interplay and implications for banking stability. In summary, the literature survey provides a comprehensive overview of the research landscape surrounding financial fraud, credit risk, and banking stability, identifying key trends and suggesting directions for future research.

2.6. Boosting Fraud Detection in Mobile Payment with Prior Knowledge

In article [6], Sun, Quan, et al. worked on the topic "Boosting fraud detection in mobile payment with prior knowledge. " *Applied Sciences* (2021): The paper titled "Boosting Fraud Detection in Mobile Payment with Prior Knowledge" by Quan Sun et al. presents a novel approach to enhance fraud detection in mobile payments, particularly targeting robotic automation. The authors propose an extended boosting machine learning model that integrates prior knowledge, such as expert rules and historical fraud data, to improve performance despite limited training data. The study demonstrates significant improvements in model accuracy, increasing from 98. 25% to 98. 71%, and recall rates from 88. 8% to 94. 8%. Key findings reveal distinct behavioral patterns between robotic and normal user transactions, including a higher jailbroken device rate (92. 47% for robotic transactions) and irregular device naming patterns. The research emphasizes the importance of combining prior knowledge with machine learning techniques to create a more robust fraud detection system and suggests future work to incorporate longer data periods and explore feature correlations for further accuracy enhancement.

2.7. Business Email Compromise Phishing Detection Based on Machine Learning: A Systematic Literature Review

In article [7], the authors Atlam, Hany F. and Olayonu Oluwatimilehin worked on the topic "Business email compromise phishing detection based on machine learning: a systematic literature review. " *Electronics* 12. 1 (2022): 42. The paper provides a systematic review of Business Email Compromise (BEC) phishing detection techniques, focusing on machine learning (ML) methods used in this area. It analyzes 38 articles selected from a larger pool, discussing their contributions and limitations. The study highlights common ML algorithms, features used for detection, and datasets employed in BEC phishing detection models. The systematic review offers a comprehensive understanding of BEC phishing detection, aiding researchers in identifying key principles and methodologies. It emphasizes the importance of developing effective detection models to combat the evolving tactics of BEC attacks. The accuracy of the proposed decision tree classification algorithms remains low, indicating a need for improvement. The algorithms face challenges such as slow convergence and long training times, which hinder their practical application. Future research should focus on enhancing the accuracy of detection models and addressing the limitations of current algorithms. There is a need to explore new features and datasets to improve the effectiveness of BEC phishing detection systems.

2.8. Introduction

In article [8], the topic “An Automated Spam Detection and Location Based Monitoring System" deals with the detection of spam. In today's digital age, the prevalence of spam calls, messages, and emails has become a significant concern for individuals and organizations alike. These unprompted communications often compromise privacy, disrupt workflows, and, in some cases, pose serious security risks, such as phishing attacks and fraud. To counter this growing menace, it is essential to adopt advanced solutions capable of detecting and mitigating spam across multiple communication channels. The Automated Spam Detection and Location-Based Monitoring System addresses these challenges by combining intelligent spam detection mechanisms with real-time location monitoring. This system leverages cutting-edge technologies in artificial intelligence, natural language processing, and geolocation services to analyze call logs, messages, and emails, classifying them as spam or genuine based on predefined patterns, keywords, and historical datasets. Once spam is detected, the system further identifies the origin of these malicious activities by tracing the sender’s location.

By integrating spam detection with location-based monitoring, this system not only enhances communication security but also provides actionable insights to trace and mitigate threats at their source. The approach is particularly beneficial in real-time scenarios, empowering users with immediate alerts and helping authorities take proactive measures against fraudulent activities. This innovative system sets the stage for a safer digital ecosystem by seamlessly combining user convenience with robust protection.

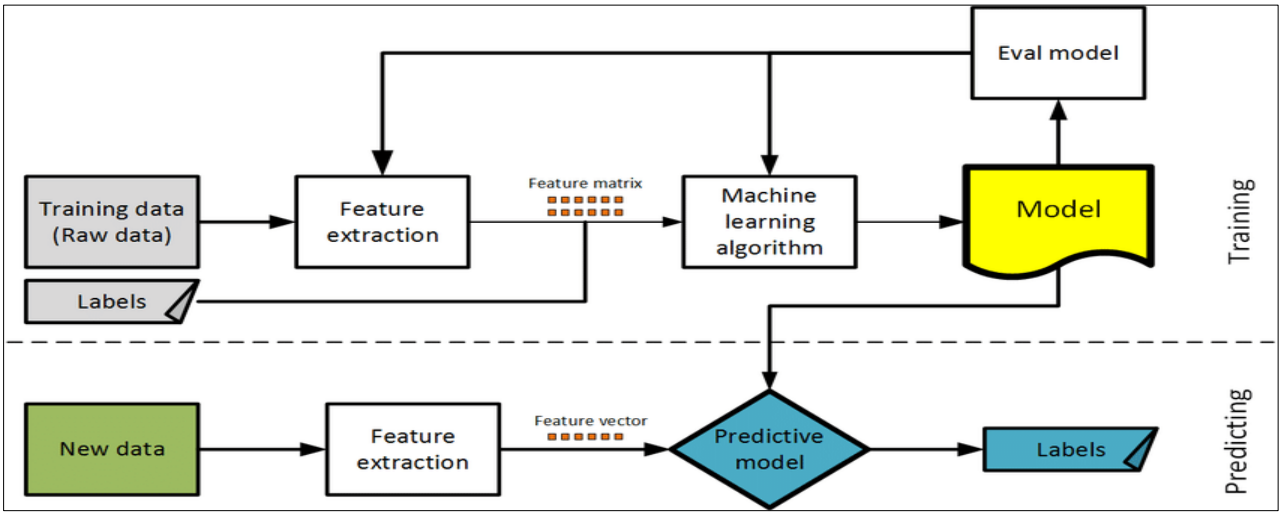

Figure 1 Overview of ml model

Spam communication — through calls, messages or emails has turned into an elaborate problem over the years, often serving as a path to other cybercrimes like phishing fraud or identity theft. And often these messages originate from unknown or remotely-blended positions. To protect the interest of individuals and organizations, a holistic solution that brings spam detection as well as source identification into play is important.

The Automated Spam Detection and Location-Based Monitoring System comprises two parts:

Spam Detection: Uses AI and machine learning software to analyze logs of calls, messages and emails to determine whether they are spam or from genuine users in real-time. By using GPS and IP tracing, you can track uses location origins of spam or suspicious activity, further enhancing accountability and security. The use of this system has proved to have various domains which include personal safety, fraud prevention and even organizational security.

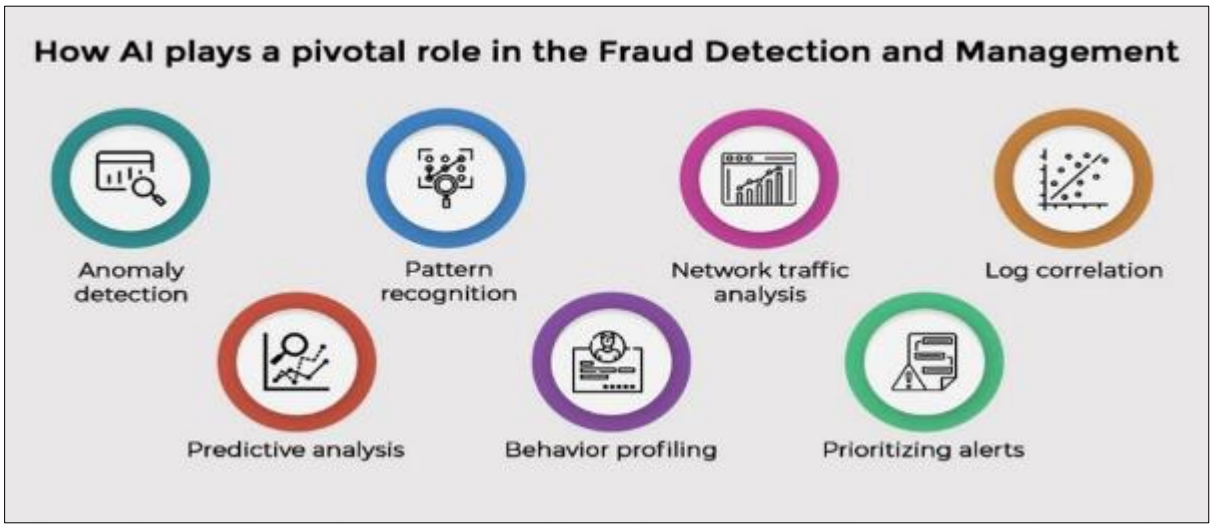

Figure 2 Role of AI in Fraud detection and Management

3. Methodology

3.1. Steps for the Flowchart

3.1.1. Data Collection

- Objective: Gather relevant data (calls, SMS, or emails) from the user for analysis.
- Steps:
  - For Mobile Number Input:
  - Fetch call logs and SMS data from the last 24–48 hours using mobile APIs or native device functionalities. Example APIs: Android Call -Log for call logs, and Content Resolver for SMS data in Android applications.
  - For Email Input:
  - Extract email content, subject lines, headers, and embedded URLs. If spam emails are hosted on services like Gmail, integrate APIs such as Gmail API.
  - If using real-time APIs: Leverage services like Twilio for communication data or VirusTotal for URL data.

3.1.2. Data Preprocessing

- Objective: Clean and normalize the data for efficient processing.
- Steps:
  - Call Logs and SMS:
    - Remove redundant entries, such as duplicate logs or repeated messages.
    - Normalize phone numbers (e.g. , convert them to a standard format with country codes).
    - Tokenize SMS or call descriptions for NLP-based analysis.
  - Email Data:
    - Parse email headers to extract sender details (e. g. , domain, IP address).
    - Remove unnecessary metadata and tokenize content for further analysis.

- Other Enhancements:
  - Remove special characters or irrelevant information.
  - Convert timestamps into a standardized format for consistent analysis.

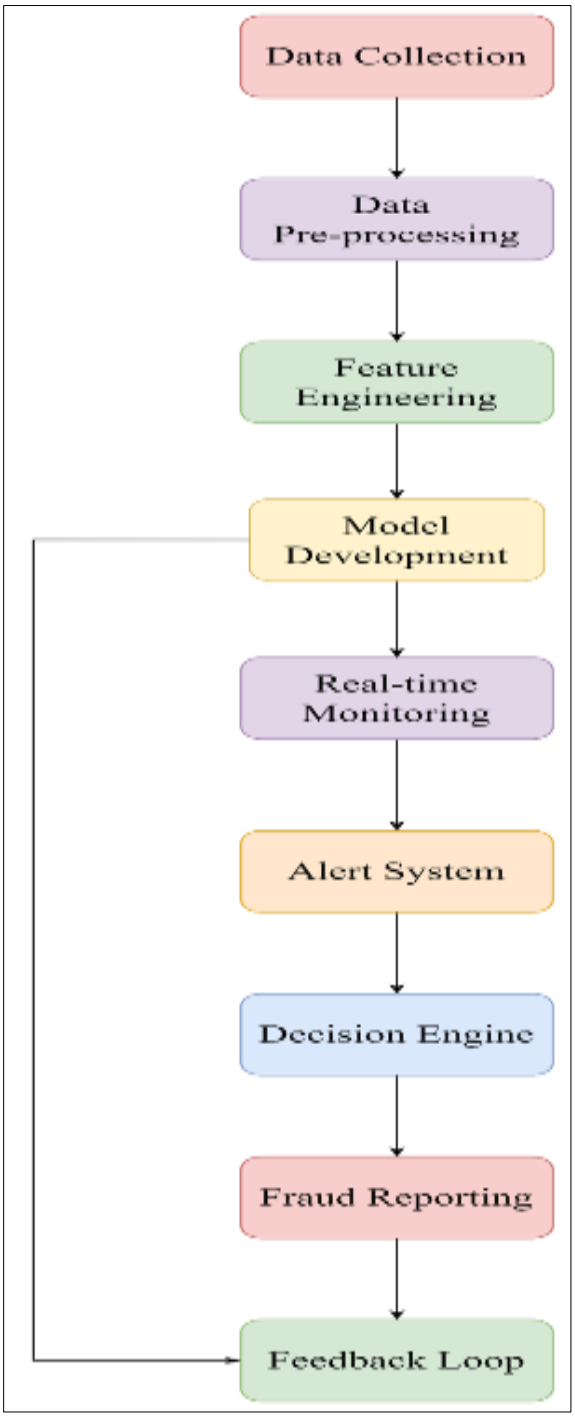

Figure 3 Block diagram of the workflow

3.1.3. Feature Engineering

- Objective: Identify and extract key patterns and information for spam detection.
- Steps:
  - Keyword Extraction: Identify common spam keywords (e. g. “lottery,” “free,” “urgent”) using text analysis tools like NLTK or SpaCy.
  - Pattern Recognition:

        - Check for repetitive patterns in sender numbers or domains.
        - Look for spam-like frequency patterns (e. g. multiple messages from unknown numbers in a short time frame).
    - Geolocation Data:
        - Extract geolocation data from device GPS (for mobile spam) or IP address analysis (for email spam).
    - Sentiment Analysis:
        - Analyze the tone of messages (e. g. overly urgent, promotional, or threatening language).

3.1.4. Model Development

- Objective: Build machine learning models for accurate spam detection.
- Steps:
    - Use datasets from sources like Kaggle or real-time spam communication logs for training.
    - Choose algorithms suitable for spam detection:
        - Traditional ML Algorithms: Random Forest, Decision Trees, or Naïve Bayes for quick and interpretable results.
        - Deep Learning Models: LSTMs or CNNs for advanced text classification, especially for email content.
    - Train separate models for:
        - Call/SMS data (focus on text patterns and phone number analysis).
        - Email/URL detection (focus on headers, links, and content analysis).

3.1.5. Spam Detection Engine

- Objective: Perform real-time classification of user inputs (calls, messages, or emails).
- Steps:
    - Integrate the trained model into a pipeline that processes user data as soon as it's received.
    - Classify each input as Spam or Genuine based on the model's prediction:
    - Calls/SMS: Detect keywords, suspicious frequency, or sender patterns.
    - Emails/URLs: Identify phishing links, malicious attachments, or spammy keywords.
    - Store classified data for further analysis and reporting.

3.1.6. Location Monitoring

- Objective: Identify the geographical origin of suspicious activity.
- Steps:
    - For Mobile Inputs:
        - Use GPS or telecom provider data to trace the physical location of the caller/sender. Example APIs: Google Maps API, Android LocationManager.
    - For Email Inputs:
        - Extract the IP address from email headers (e. g. , Received-SPF, X-Originating-IP) and map it using geolocation APIs like MaxMind ,GeoIP or ipapi.
        - Present the location on a visual map for better user understanding.

3.1.7. Alert System

- Objective: Notify users about detected spam in a clear and actionable way.
- Steps:
    - Generate Spam Report:
        - Include detailed information about detected spam, such as:
        - For calls/SMS: Numbers flagged as spam, message content, timestamps.
        - For emails: Sender details, flagged content, malicious links.
    - User Notifications:
        - Notify users via the app or system with alerts showing spam summaries.
          Example: "5 spam messages detected. Click to view details. "
        - Provide actionable steps like marking messages as safe or reporting them.

3.1.8. Decision Engine

- Objective: Empower users to customize spam detection settings.
- Steps:
    - Allow users to:

- Whitelist trusted phone numbers, email addresses, or domains to avoid false positives.
- Blacklist suspicious entities permanently for stricter filtering.
- Provide adjustable thresholds for spam classification sensitivity.

3.1.9. Fraud Reporting

- Objective: Enable users to take corrective action against detected spam.
- Steps:
  - Generate detailed fraud reports with evidence (e. g. , spam message content, geolocation).
  - Allow users to report spam to:
    - Telecom providers for call/SMS-based spam.
    - CERT (Computer Emergency Response Team) or email service providers for phishing emails.
    - Facilitate automated reporting via integrated APIs for faster action.

3.1.10. Feedback Loop

- Objective: Continuously improve the detection system.
- Steps:
  - Collect user feedback on false positives or missed spam cases.
  - Use this feedback to retrain the ML models with updated patterns.
  - Periodically update keyword databases and detection thresholds based on emerging trends.

4. Results and discussion

4.1. Step 1: In the first step, run your application. Once it starts, a port number will appear. By clicking on this port, the home page will be generated

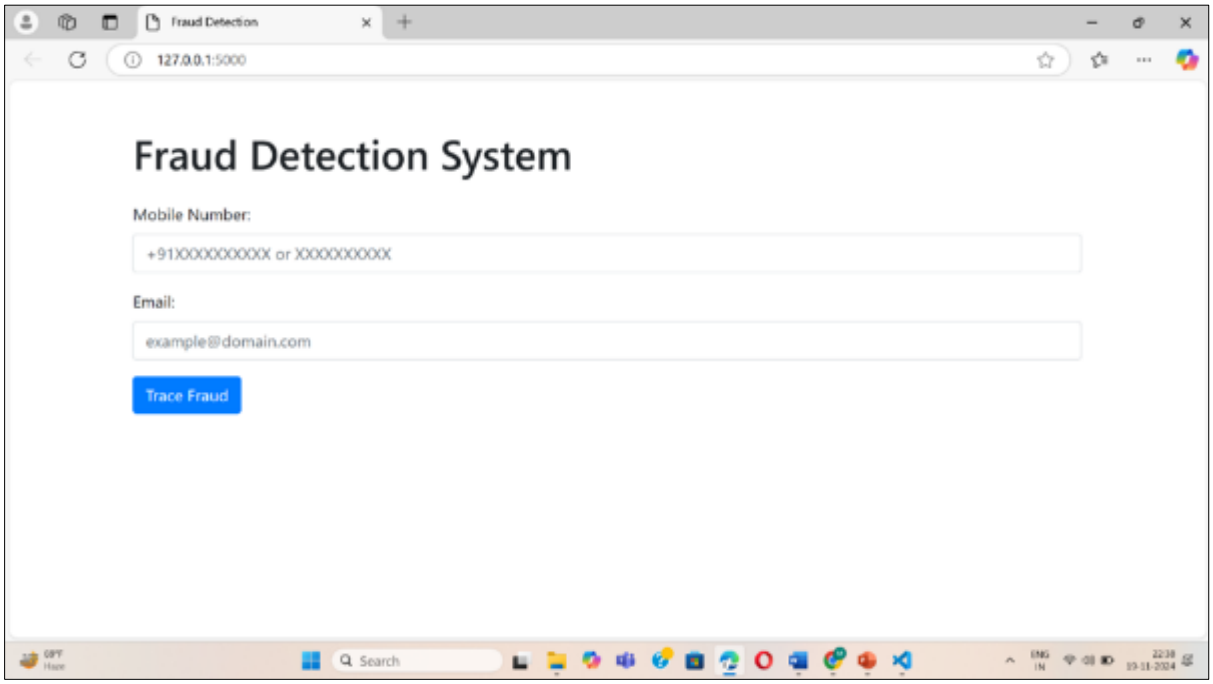

Figure 4 Home page

4.2. Step 2: Enter the required inputs.

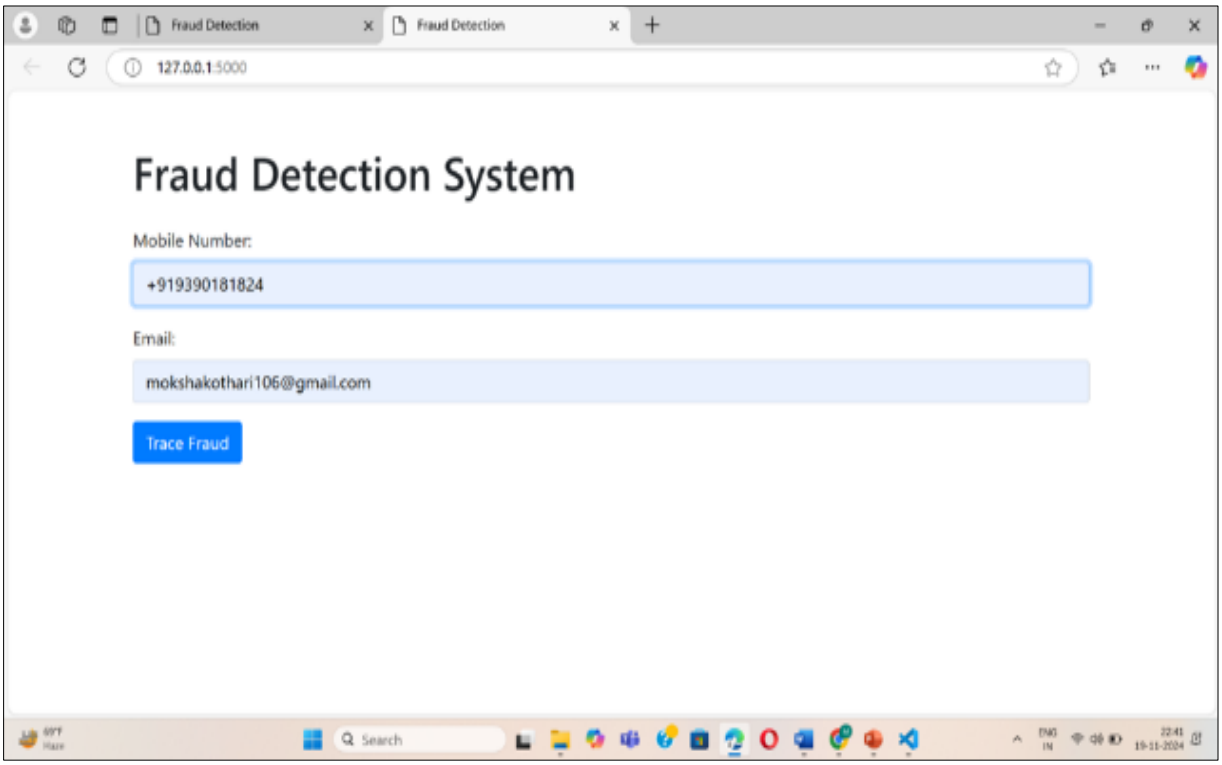

Figure 5 Fill the user input

4.3. Step 3: Once the required input fields are filled, click on trace fraud.

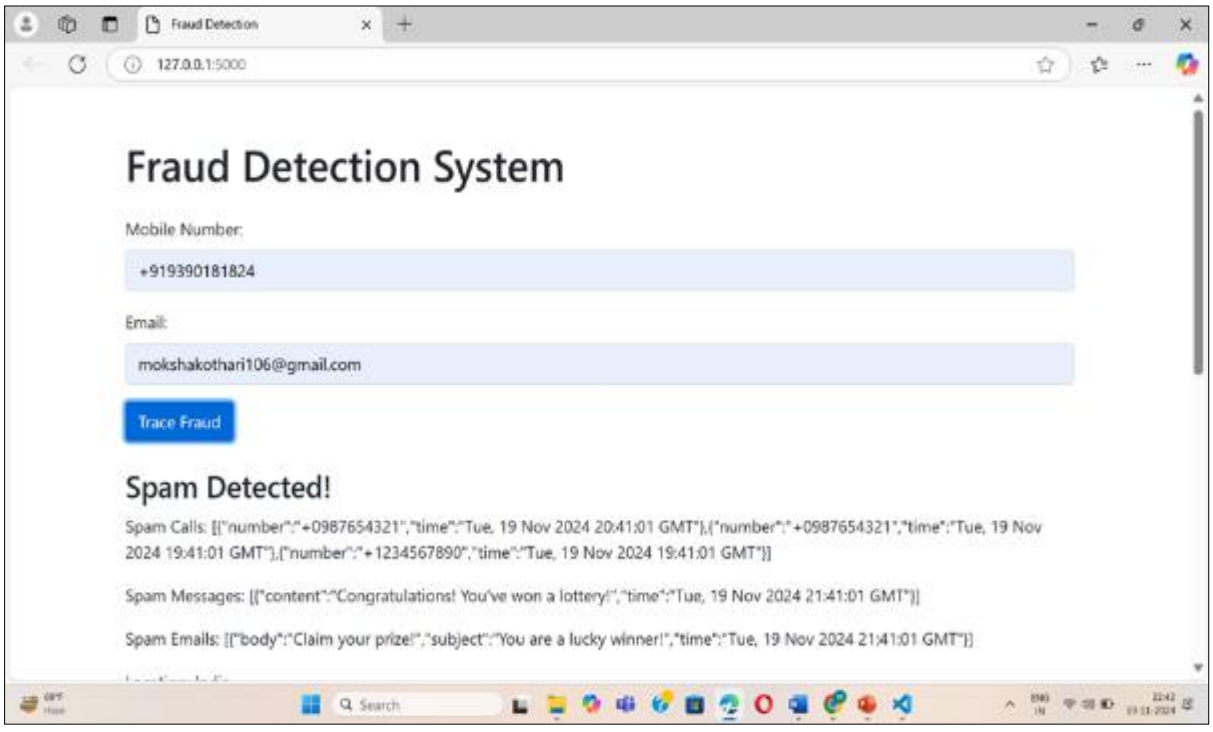

Figure 6 Displaying the spam detected

4.4. Step 4: The results will be displayed as shown.

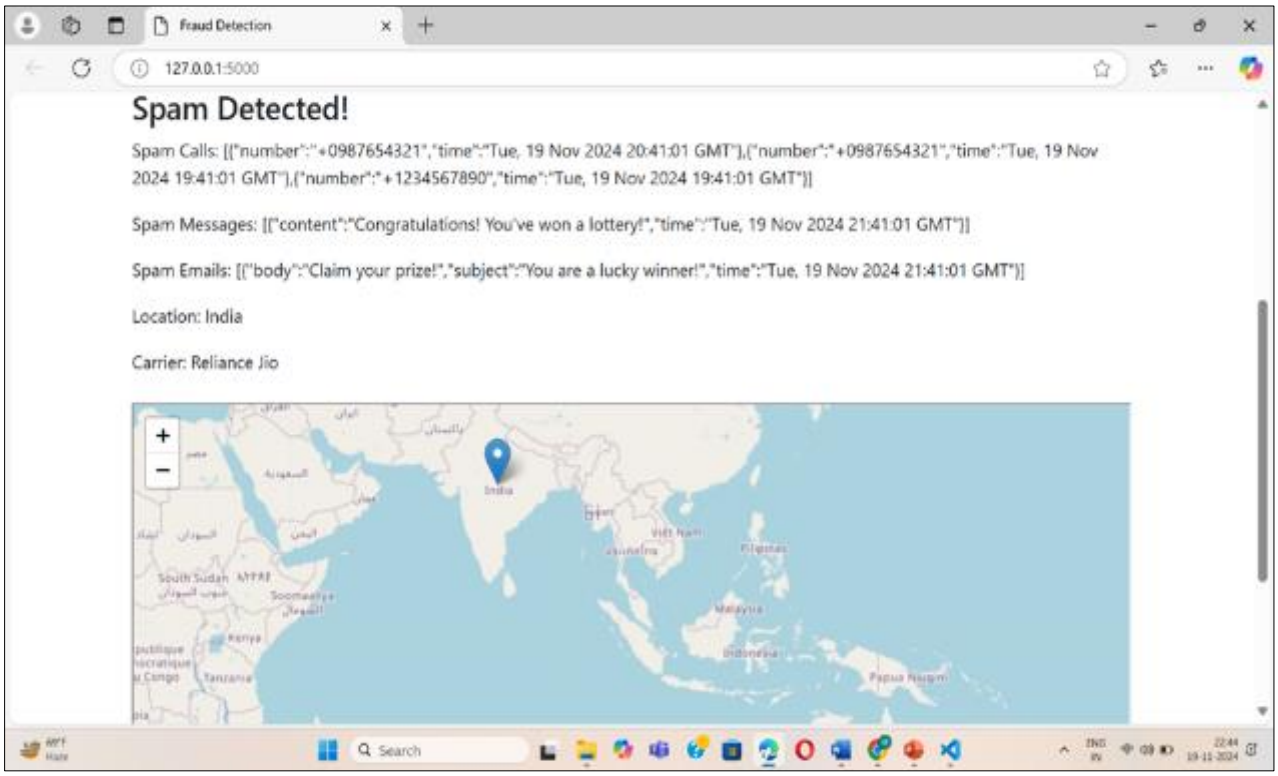

Figure 7 Spam Detection Location

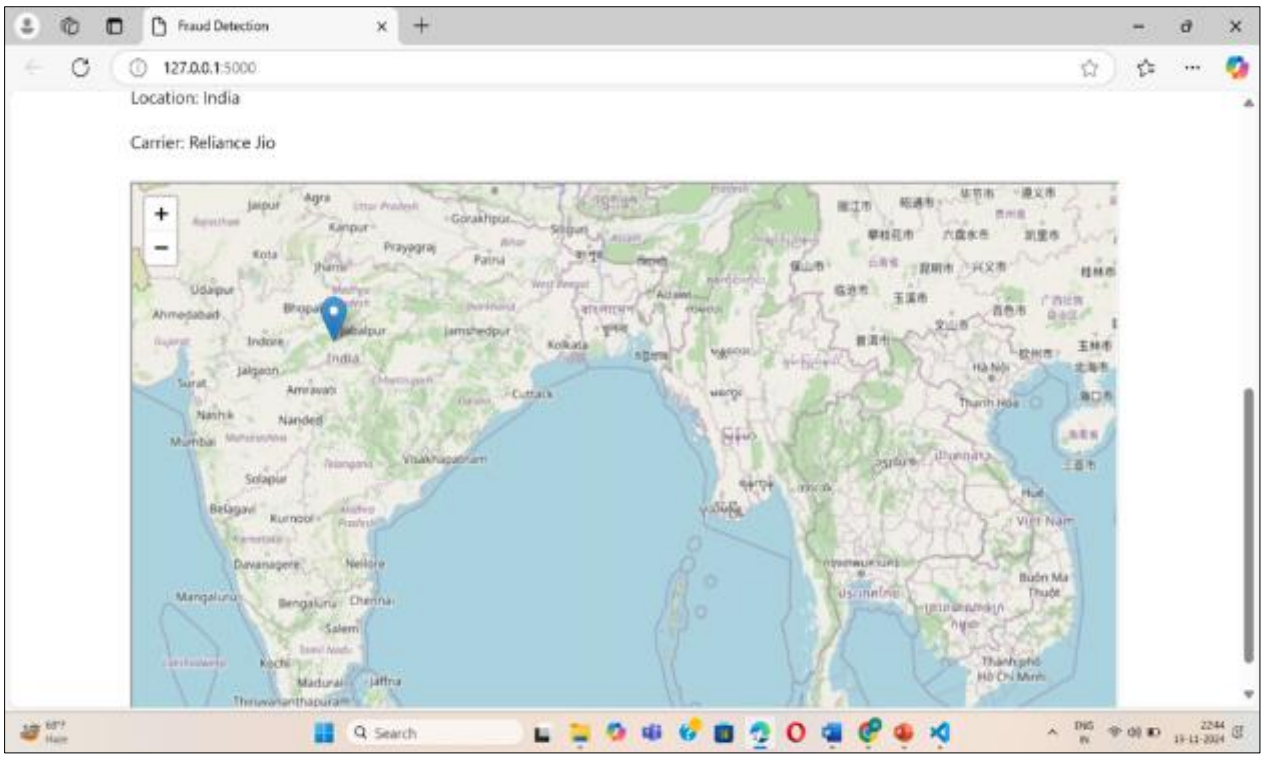

Figure 8 Tracing the location

5. Conclusion and Future scope

This project is an initial spam detection and locality tracing model based on a sample dataset with mock data. Later on, to setup this system as a real-time application, we can acquire suitable permissions & integrate with telecom operators, email service providers and advanced geolocation APIs. The system uses advanced machine learning models trained on large datasets to dynamically adjust to worldwide spam trends and enhance the accessibility of scam detection. Adding support for various languages and behavioral analysis can make it useful in different regions. Moreover, the implementation of comprehensive privacy and security measures, including end-to-end encryption allows protecting data as well as providing access to call logs, messages and emails in real-time. If the powers to be suits together with the aversion trick specialists, the system can transform into a weapon in culmination against spam and fishing on big scale. Offering cross-platform support, advanced reporting dashboards and enterprise-level customization, the application can provide both individual users and businesses a scalable and effective solution for spam and fraud detection in communication networks.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Wadha, A, Somaya, M. , Abdulghani, A. , & Muhammad, K. (2020). Comprehensive review of cyber crime detection techniques. Proceedings of IEEE Access, Special Section on Emerging Approaches to Cyber Security, 1-19.

[2] Azam, Hamza, et al. "Cybercrime Unmasked: Investigating cases and digital evidence. " International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence 2. 1 (2023).

[3] Shulha, Olha, et al. "Banking information resource cybersecurity system modeling. " Journal of Open Innovation: Technology, Market, and Complexity 8. 2 (2022): 80.

[4] Afjal, Mohd, Aidin Salamzadeh, and Léo-Paul Dana. "Financial fraud and credit risk: Illicit practices and their impact on banking stability. " Journal of Risk and Financial Management 16. 9 (2023): 386.

[5] Sharabov, Maksim, et al. "Filtering and Detection of Real-Time Spam Mail Based on a Bayesian Approach in University Networks. " Electronics 13. 2 (2024): 374.

[6] "Stabek, Amber, Paul Watters, and Robert Layton. "The seven scam types: mapping the terrain of cybercrime. " 2010 Second Cybercrime and Trustworthy Computing Workshop. IEEE, 2010. Electronics 13. 2 (2024): 374

[7] Mughaid, Ala, et al. "A novel machine learning and face recognition technique for fake accounts detection system on cyber social networks. " Multimedia Tools and Applications 82. 17 (2023): 26353-26378.

[8] Sun, Quan, et al. "Boosting fraud detection in mobile payment with prior knowledge. " Applied Sciences 11. 10 (2021): 4347.