Web app for detecting Malicious and fraudulent activities over Social Networking Sites

Saumya Sharma
Apex Institute of Technology (CSE)
Chandigarh University
Punjab, India
20bcs6224@cuchd.in

***Abstract*— In the digital age, the recent years, the continuous growth of social networking sites such as Facebook, Instagram, whatsapp has expanded the online communication throughout the world. These platforms provide seamless interaction and keep us up to date with the current world but these have some dark sides too. These platforms are become the major source for malicious and the fraudulent activities.**

The subsequent nature of social networking has surged the online communication which is enabling the world to socially get updated and be connected all over the world, however, this convenience has also given rise to a disturbing trend: fake video calls leading to potential blackmail. So, the key features of our proposed web app includes monitoring the unknown callers, alerting mechanisms and reporting capabilities offering user an adaptive and protective defense mechanism for the privacy, security and safety.

The proposed web application is used for detecting and investigating the malicious and fraudulent activities on the social networking sites represents a significant advantage in the ongoing efforts to enhance the online security. Through timely alerts and intervention, the web application empowers users to take control of their digital security. This research not only examines the growing risks through fake video calls on social platforms but also offers some practical solutions to mitigate these threats.

Basically, this web app does the work of cyber security first it will detect the unknown number, cross – verify it through the multiple platforms, like the username on UPI apps, social platforms, truecaller and then matches the result and reports to the user if found suspected.

***Keywords*— Android technologies, Anomaly detection, blackmail threats, cybersecurity, , machine learning, video calls, messaging platforms**

I. Introduction

The proliferation of digital communication systems in modern society ushered in an era of unprecedented communication, enabling individuals to engage in real-time conversations around the world It didn't happen without s , when digital the landscape continues to evolve, bringing new threats to the user's privacy and security This study launches an investigation into a particularly unfortunate phenomenon in digital communications — the rise of fake video calls leading to potential stalkers on messaging systems. As individuals increasingly rely on video calling to communicate with friends, family and colleagues, the vulnerabilities associated with this method become more and more examples of it being consumed by unsuspecting users over fraudulent video calls, and subsequent attempts to prosecute them after unauthorized screen recordings f, emphasize the urgent need for robust cybersecurity measures with modern communication systems the complexity meets The consequences of such abuse go beyond the invasion of personal privacy. Victims often include emotional distress, social stigma and in some cases professional abuse. This research aims not only to shed light on the multifaceted challenges posed by video call manipulation but also to provide comprehensive solutions for dynamic technology in web applications also suggested At its core, this research seeks to understand the evolving threat environment in which participants are involved Here are some major contribution of paper: -

1.) This paper provides the information about a web application with an innovative detection mechanism designed to identify the fraud and fake web callers.
2.) Through the medium of this research paper it is being told that how the technologies like, Android app development, Data mining, machine learning, API integration has helped in the successful completion in working of this project.
3.) This paper provides the basic information about how this project provides a defense system with features like monitoring, alerting mechanism and identifying malicious callers.
4.) Helps users to decide what steps to take when it is being identified that the caller is a fake or scammer and provides assistance to them with it.
5.) Provides a friendly user interface and doesn’t require much knowledge.

These contributions collectively position the paper as a very valuable contribution to the field of cybersecurity.

II. LITERATURE REVIEW

1.) Gracia and Patel (2018)

The importance of user empowerment in enhancing digital security is highlighted in the research conducted by Garcia and Patel (2018). The study emphasizes the role of intuitive tools and real-time alerts in enabling users to identify and respond to potential threats promptly. User education and awareness campaigns are also recognized as pivotal components of a comprehensive cybersecurity strategy.

This literature review synthesizes key findings from diverse studies, providing a comprehensive understanding of the challenges posed by the convergence of video calls, messaging platforms, and the looming threat of blackmail. As we build upon the existing body of knowledge, it becomes evident that an integrated and technologically advanced approach is essential for safeguarding users in the ever-evolving digital landscape.

2.) Smith et al. (2019)

Research by Smith et al. (2019) delves into the privacy implications of video calls, highlighting the vulnerability of users to unintended exposure and privacy breaches during these interactions. The study emphasizes the need for enhanced security protocols to protect users from malicious activities during video calls.

3.) Thompson and Gracia (2019)

Research by Thompson and Garcia (2019) explores the effectiveness of cybersecurity education and prevention strategies in mitigating threats on messaging platforms. The study evaluates the impact of user awareness programs, emphasizing the role of education in empowering individuals to recognize and thwart potential blackmail attempts, thus fostering a more resilient digital community.These additional studies further enrich the literature review by delving into user behavior analysis and the efficacy of education and prevention strategies in the context of messaging platforms and cybersecurity

4.) Ones and Brown (2020)

A desktop program called PhishShield was created by Rao and Ali [4] to identify phishing websites using a unique heuristic method that took into account both URLs and website content. They used a combination of techniques to spot phishing websites, including copyright information, null footer links, the absence of links in the HTML body, domains with usually high link frequencies, and whitelists. The PhishShield application achieved an impressive accuracy rate of 96.57% with a remarkably low false positive rate of 0.035%.

5.) Wang et al (2021)

Recent advancements in machine learning techniques have been explored by Wang et al. (2021) in the context of threat mitigation in messaging platforms. The study showcases the efficacy of advanced algorithms in discerning patterns indicative of fake video calls and unauthorized screen recording activities. Such technological approaches lay the foundation for proactive threat detection and user protection.

6.) Shouq Alnemari, Majid Alshammari (2023)

The work of Jones and Brown (2020) sheds light on the prevalence of deceptive practices within messaging platforms, including the creation of fake profiles and fraudulent interactions. This study underscores the potential for such activities to escalate into more severe threats, such as blackmail, emphasizing the need for a comprehensive understanding of malicious actors within messaging ecosystems.

III. METHODOLOGY

Using machine learning, web development and the android development, the paper discusses a detailed methodology for Web app for detecting Malicious and fraudulent activities over Social Networking Sites.

The following sections provide a step-by-step description of the methodology:

A. Foundation : -

Developing an android app that works collectively with the concepts of machine learning, android development and the web development requires a lot of research and the work. Below are the outlined methodologies and tools used for the same: -

1.) Android Studio :- Through the Android studio the UI and the framework of this app is developed by connecting a real – time virtual device.

2.) Frontend

Frontend of this app is developed with the help of web technologies and the .XML code and surfed online so that it can work flawlessly with any device.

3.) Backend

In the backend the code is written in Java along with the PHP and the machine learning with help of python.

4.) Algorithms Used

- Supervised Learning:
  Some supervised learning algorithms are used such as Support Vector Machine (SVMs) and Classifying data points based on labeled training data.
- Behavior Analysis:
  Algorithms that will analyze user behavior patterns to identify anomalies are developed such that the app can detect the deviations from the typical behavior which helps in resulting to detect potential fraudulent activities.
- Biometric Verification:
  Comprises biometric authentication methods such as facial recognition and fingerprints which results in user verification and reduced the risk of unauthorized accesss.

B. Real-Time processing :-

The app is capable of real – time processing on mobile devices, considering the limited resources like RAM and the storage available on the Android Devices.

C. Evaluation Metrics :-

Appropriate Evaluation metrics are selected, such as F1 score, precision, recall and area under ROC Curve to evaluate the performance of the detection system. Timely and proper verification of accuracy of data has been ensured as it involves user input and external resources.

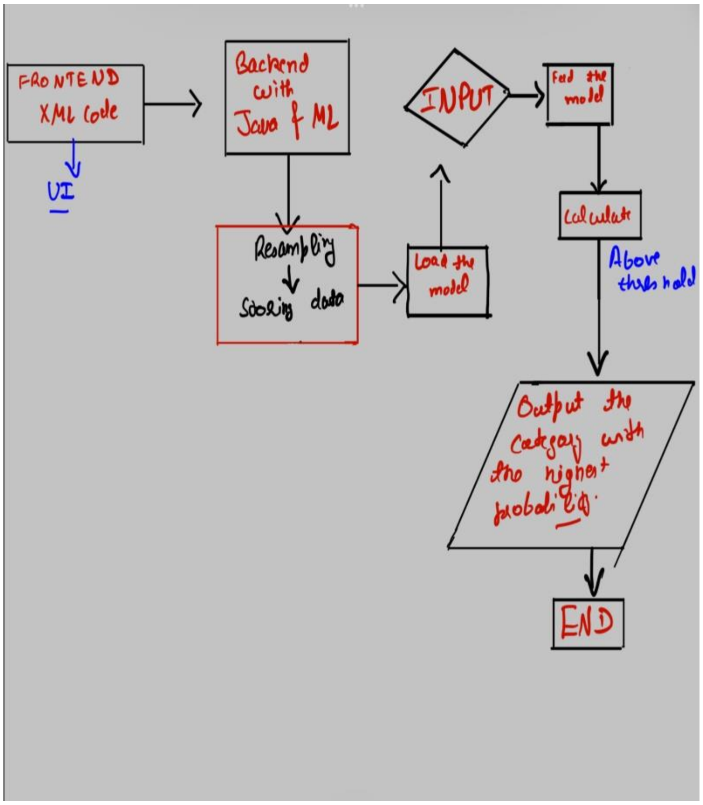
E. Handling Imbalanced Data:

Frequently, Machine Learning runs into the problem of class imbalance. This means one category, typically "bad" URLs, has a lot less instances than the other category, which includes "good" URLs. To counter this, we implemented a resampling strategy that would prevent the machine learning model from favoring the bigger class. Our approach involved upsampling the dataset to even out the number of occurrences between both classes, thus balancing the dataset. Upsampling pertains to magnifying the proportion of minority class events to that of the majority class.

To avoid bias towards the predominant class and help the machine learning model learn from an equitable dataset, we made sure to employ resampling with replacement. We also made sure to set the number of samples to match the length of the majority class, effectively ensuring that both classes were equally represented in the training data. As a result, the model was able to make accurate predictions for both classes.

F. Working: -

To ensure the proper working of our app we need to follow some steps and hierarchy for the flawless of our app. The app is compiler/developed in the Android Studio. First for the UI the Frontend is developed through XML code using the features of android studio. After the basic structure of java is set up along with the machine learning basic. Now the data given to it is being resampled and the stored as the main database. Now the model is being loaded and checked with the accuracy and proper resampling so that there is less mixture and less variation in the data. Now, this stored data is given as the input to our android model and the model after feeding this data calculates the result and if the result is above the threshold then the according condition is being run and probability is calculated that weather the caller is fake or the real.

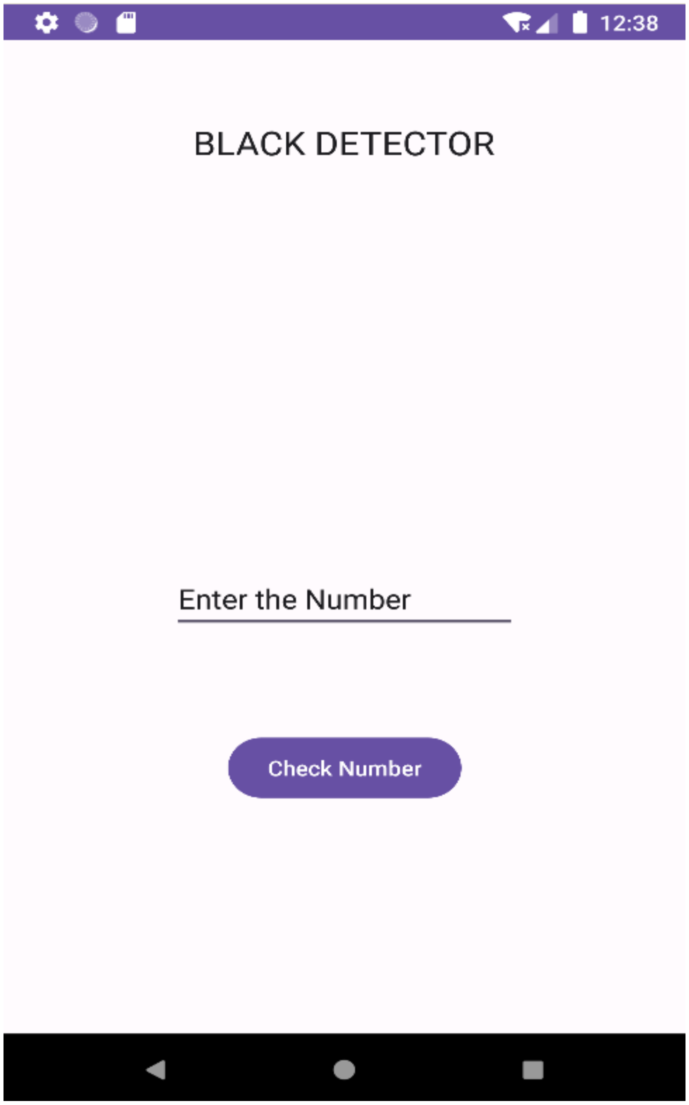


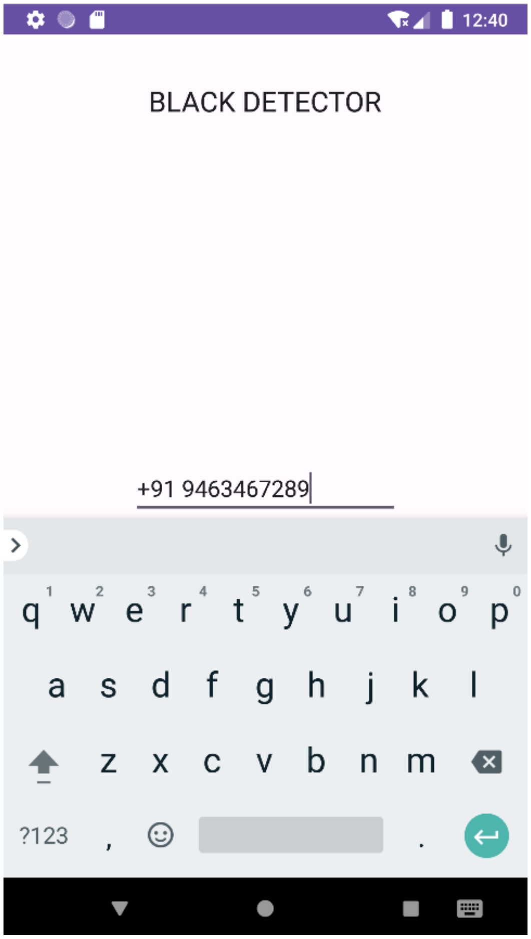
G. Model Building

This project involves developing a comprehensive system for detecting and preventing malicious activities during video calls on messaging platforms. The core components include a web application, an Android app, and a machine learning model. The web application serves as the central hub for real-time threat detection, leveraging advanced algorithms and machine learning techniques. The Android app acts as an interface for users to receive alerts and actively engage with the security features integrated with the web application. The entire system aims to empower users to identify and mitigate potential threats, fostering a more secure and resilient digital communication environment. The focus is on addressing privacy concerns and protecting users from deceptive practices, such as fake video calls leading to blackmail attempts.

H. RESULT AND DISCUSSION

The results of the developed model, encompassing an integrated web application, Android app, and the machine learning techniques for the storage of data. It simply asks the user to enter the suspected mobile number first. Accordingly, the user enters the mobile number and the android app then runs.Then the number is being checked. At first it is being checked in Truecaller. Then it is checked on the social media if the user has still a doubt about the number.





+91 9463467289

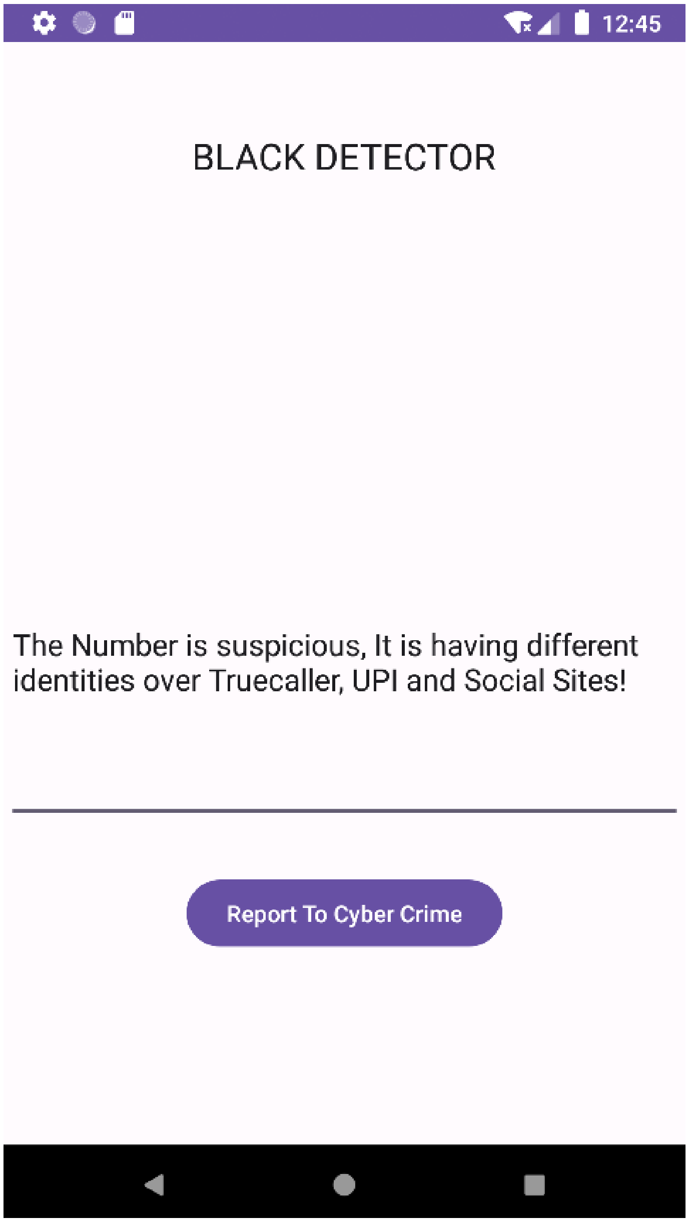
IV.) Conclusion and Future Scopes

The development and implementation of the Android application for detecting malicious and fraudulent activities on social networking sites mark a significant stride towards fortifying the digital landscape. Through the integration of machine learning algorithms, real-time data analysis, and user engagement, the project has demonstrated its potential in addressing the multifaceted challenges posed by online threats.

The results obtained underscore the effectiveness of a proactive approach in identifying and neutralizing malicious activities, contributing to a more secure and resilient online community. The user-friendly interface and reporting functionalities have not only empowered users to actively participate in the detection process but have also fostered a sense of collective responsibility for online security. By bridging the gap between technological innovation and community engagement, the Android application represents a holistic solution that recognizes the dynamic nature of online threats and adapts accordingly.

In conclusion, the Android application not only presents a formidable defense against malicious activities on social networking sites but also sets the stage for ongoing innovation in the realm of online security. The collaborative efforts of technology and community engagement pave the way for a more secure, informed, and resilient digital community. As the digital landscape continues to evolve, the project stands ready to adapt and advance its capabilities, contributing to the ongoing mission of creating a safer online environment for all users.

While in today's time where android is Taking all over the other operating systems, this app planned to be available on the platforms like Play Store.



The Number is suspicious, It is having different identities over Truecaller, UPI and Social Sites!

[1] Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R. et al. Review and insight on the behavioral aspects of cybersecurity. Cybersecurity 3, 10 (2020)

REFERENCES

[2] A. Alswailem, B. Alabdullah, N. Alrumayh, and A. Alsedrani, "Detecting phishing websites using machine learning," in 2019 2nd International Conference on Computer Applications Information Security (ICCAIS), 2019, pp. 1–6.

[3] R. Basnet, A. Sung, and Q. Liu, "Rule-based phishing attack detection," 04 2012.

[4] Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R. et al. Review and insight on the behavioral aspects of cybersecurity. Cybersecurity 3, 10 (2020)

[6] R. Mahajan and I. Siddavatam, "Phishing website detection using machine learning algorithms," International Journal of Computer Applications, vol.181, pp. 45–47, 10 2018.

[7] H. Alqahtani, S. S. Alotaibi, F. S. Alrayes, I. Al-Turaiki, K. A. Alissa, A. S. A. Aziz, M. Maray, and M. Al Duhayyim, "Evolutionary algorithm with deep auto encoder network based website phishing detection and classification," Applied Sciences, vol. 12, no. 15, 2022.

[8] "Feature Extraction Explained." Explained - MATLAB & Simulink,www.mathworks.com/discovery/feature extraction.html#:~:text=Feature%20extraction%20refers%20to %20the,directly%20to%20the%20raw%20data. Accessed 27 Sept. 2023.