

# Challenge - Fraud App Detection

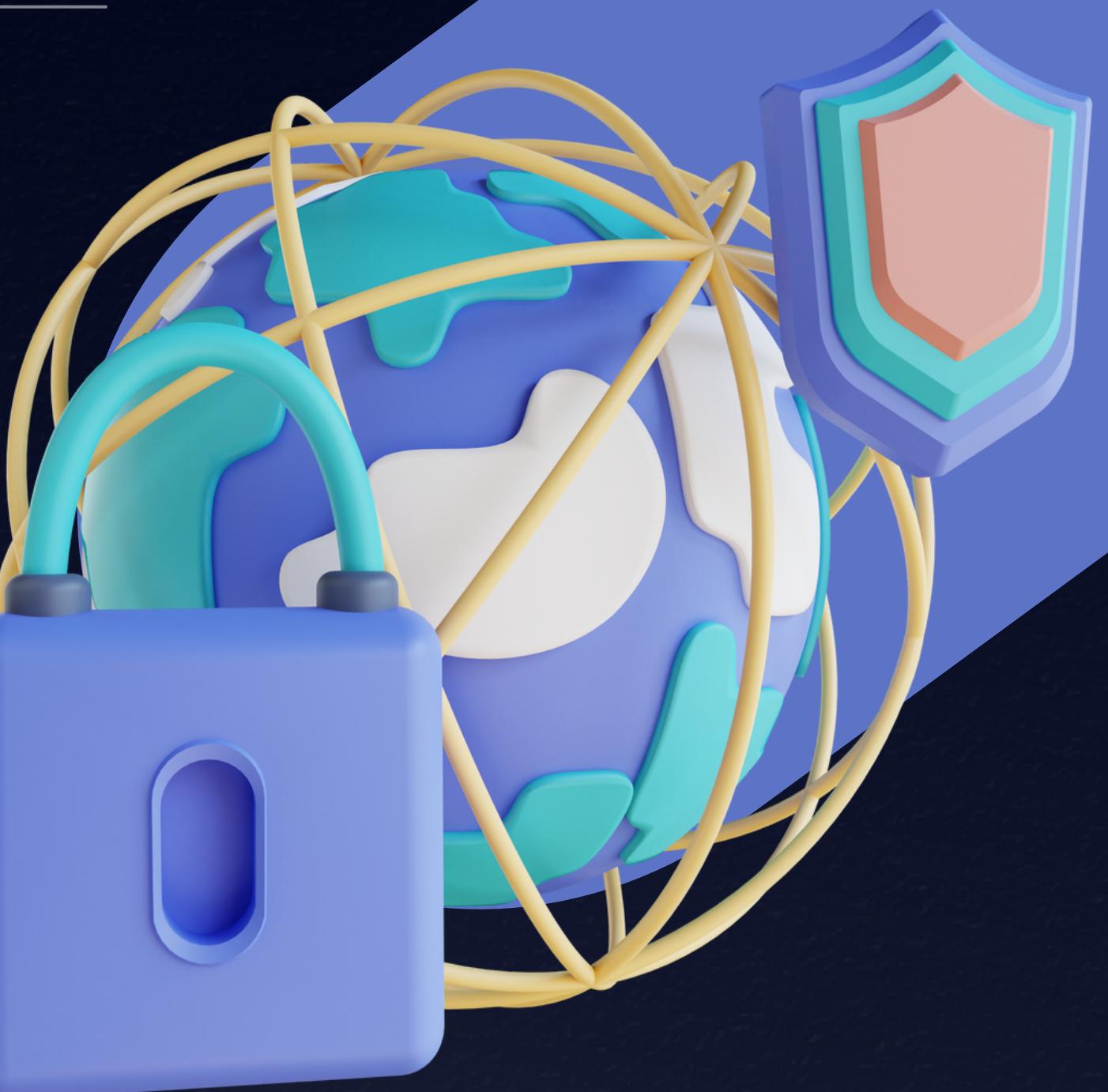
---

## Team - TeamCode

Team Members :

Deepakshi Mahajan  
Shashank Mangal  
Shubham Mehla  
Ashish

Get Started



# What are Fraud Apps ?



Fraud apps are designed to deceive or defraud users. These apps can take many forms, such as apps that steal personal or financial information from users, apps that contain malware or other harmful code, or apps that charge users for services or products without their knowledge or consent. They may be available on app stores or other platforms, and they can be difficult to identify because they are often disguised as legitimate apps.



Introduction →

# Problem Statement



Fraud apps are a growing problem that can harm both app developers and users.

These apps can steal personal and financial data, spread malware, and charge users for services without their knowledge, leading to identity theft, financial loss, and damage to the reputation of app stores and platforms.

In this presentation, we will explore the various forms that fraudulent apps can take and discuss ways to identify and protect against them.

# Our Solution

- So keeping all this in mind we have designed a web app "**FRAUDWAR**", an AI-powered Fraud Detection and Scanning Android App to prevent users and firms from continuously happening frauds and malware works.
- The app will automatically scan the malfunctioning activities with the help of developer's track and the metadata of the application.

Our Solution





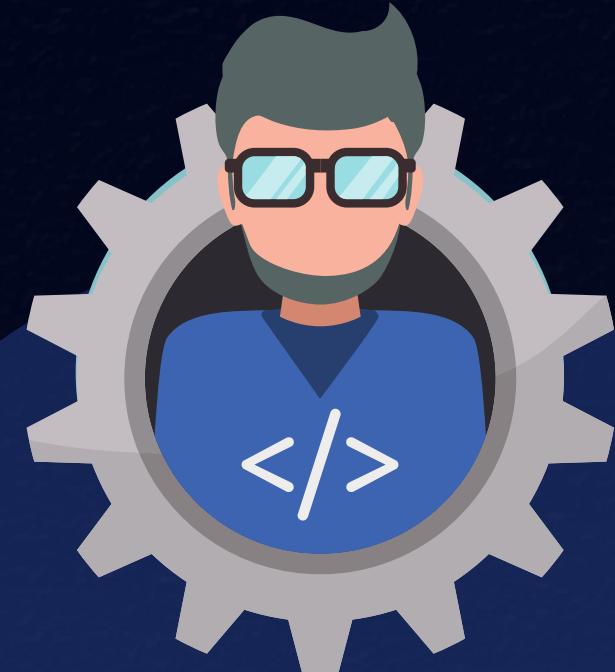
## Analyze app metadata & code

The metadata and code of an app, such as its description, developer information, and screenshots, can be analyzed to identify patterns of fraud or malicious intent. Ex: Phishing site links in the code, apps with incomplete or misleading descriptions, etc.



## Check app permissions

The permissions requested by an app can also be evaluated to determine whether they are right, reasonable and necessary for the app's intended functionality. Unreasonable or unnecessary permissions may be a sign of fraud or malicious intent.



## Monitor developer activity

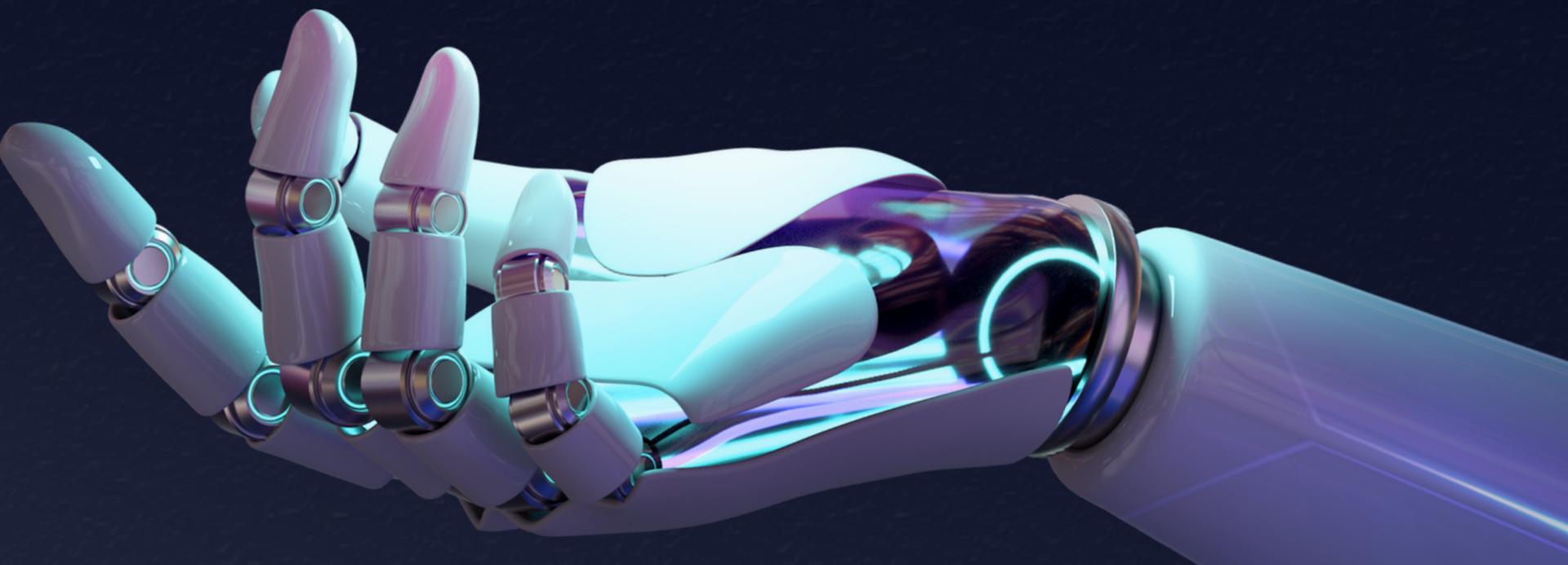
The activity of developer can be monitored to identify patterns that are indicative of fraud or any malicious intent.

Ex: developers submitting many apps in a short time, or having a history of fraud, may be more likely to be involved in fraud apps.

# Why are we different ???

Our AI-powered fraud detection app stands out from others as it includes the use of advanced machine learning algorithms, real-time monitoring and alerts, integration with other security systems, and a user-friendly interface. It can be used to analyze historical data on fraud incidents, identify patterns and characteristics that are indicative of fraudulent activity, and build a model that can be used to predict the likelihood of future fraud.

Difference



# List of the features offered by the app



## Data Analysis

The app would use machine learning algorithms to analyze the data and metadata of apps, looking for patterns or anomalies that might indicate fraudulent behavior.



## Notification Alert

The app would send notifications to users when a potentially fraudulent app is detected, either on the user's device or in an app store or platform.



## User Reporting

The app would allow users to report suspicious apps, either by submitting a report through the app or by flagging an app for review.



## Security Tips

The app would provide users with tips and best practices for protecting against fraudulent apps, such as only downloading apps from reputable sources.

# Business Logic of the Solution



## Charging for app scanning

One option is to charge users a fee to scan their apps for malware and other threats. This could be a one-time fee or a subscription-based model.



## Revenue through Advertising

Another possibility is to generate revenue through advertising. The app would display ads to users, either while they are using the app or as notifications.



## Partnerships and referrals

The app can generate revenue through partnerships with app stores or other platforms, or by referring users to these platforms to download apps.

# Technology Used

- Web scraping tools
- Machine learning libraries such as TensorFlow, Scikit-learn, and Keras
- Java, kotlin, and XML for App development
- Android Studio
- Firebase
- Database Technology MySQL
- Visual Studio Code
- Jupyter Notebook



# THANK YOU!

