BENNETT UNIVERSITY
TIMES OF INDIA GROUP

FAKE ACCOUNT DETECTION

USING MACHINE LEARNING

Submitted To-: Dr. Yajnaseni Dash

BENNETT UNIVERSITY
TIMES OF INDIA GROUP

TEAM

NITYA GOEL
E23CSEU0317

SAMYA GUPTA
E23CSEU0329

MRIGASHI
E23CSEU0327

INTRODUCTION

These days, almost everyone uses social media or online platforms to connect with others. But along with real users, there are also fake accounts that people create to do harmful things like spreading false information, sending spam, cheating others, or even hacking. These fake profiles can cause a lot of problems and make online spaces less safe. So, in this project, we tried to build a simple system using programming and machine learning that can spot fake accounts. The main goal is to help make social media platforms safer and more trustworthy for everyone.

PROJECT OBJECTIVES

Build a Detection Model

Develop a machine learning model that can automatically identify and flag fake accounts based on selected features.

Minimize Spam and Fraud

Help reduce spam, scams, and malicious activity on online platforms by filtering out suspicious users.

Solve a Real-World Problem

Apply machine learning techniques to tackle a real-world cybersecurity issue and make digital spaces safer.

TOOLS AND TECHNOLOGIES

We used the following tools and libraries:

- Python – Core programming language
- Pandas & NumPy – Data handling and preprocessing
- Scikit-learn – Training and testing ML models
- Matplotlib – Visualizing results
- Jupyter Notebook – Developing and testing the solution interactively

DATA COLLECTION

- We collected sample datasets from platforms like Kaggle.
- The dataset contained user account information such as:
- Date of account creation
- Number of posts, followers, and following
- Frequency of activity
- Whether profile picture, bio, or other fields were filled

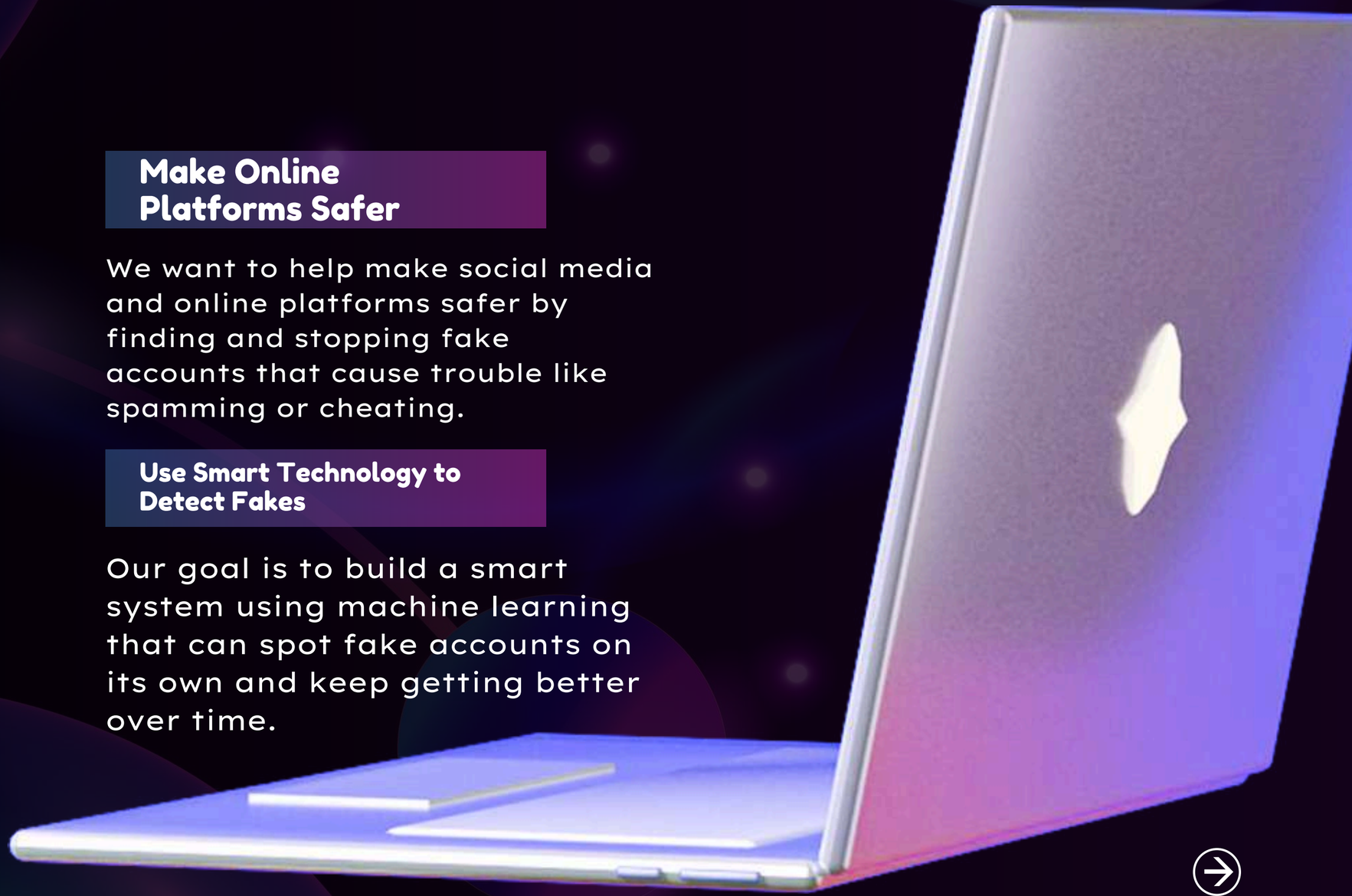
OUR VISION

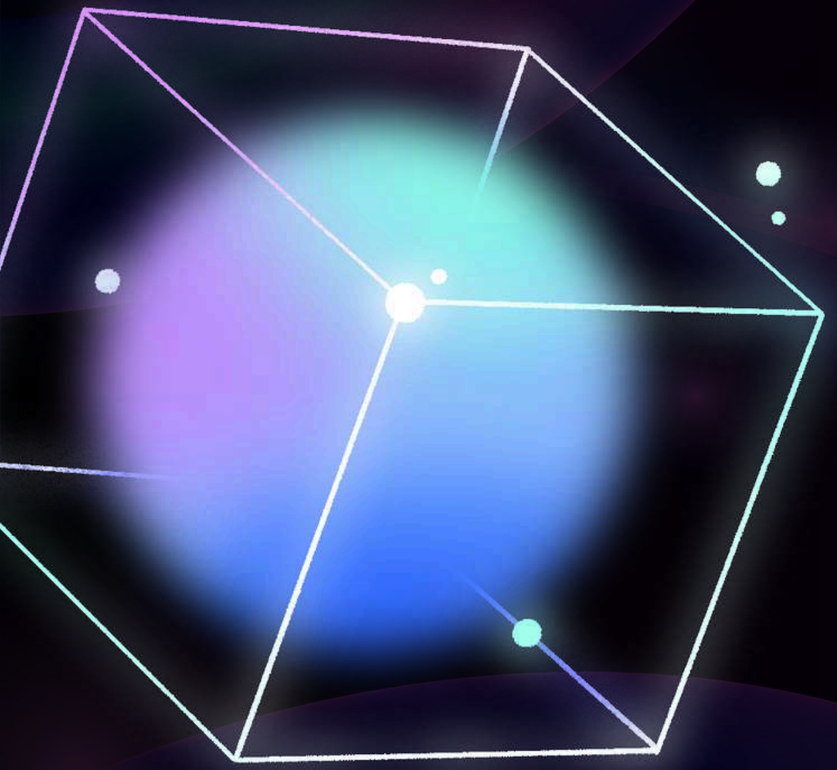
Make Online Platforms Safer

We want to help make social media and online platforms safer by finding and stopping fake accounts that cause trouble like spamming or cheating.

Use Smart Technology to Detect Fakes

Our goal is to build a smart system using machine learning that can spot fake accounts on its own and keep getting better over time.





FEATURE SELECTION

Incomplete or Suspicious Profiles

Fake accounts often have missing profile pictures, bios, or other key details.

Unusual Activity Patterns

They may post the same thing repeatedly or show sudden spikes in activity.

Follower-Following Imbalance

These accounts usually follow many users but have very few followers in return.

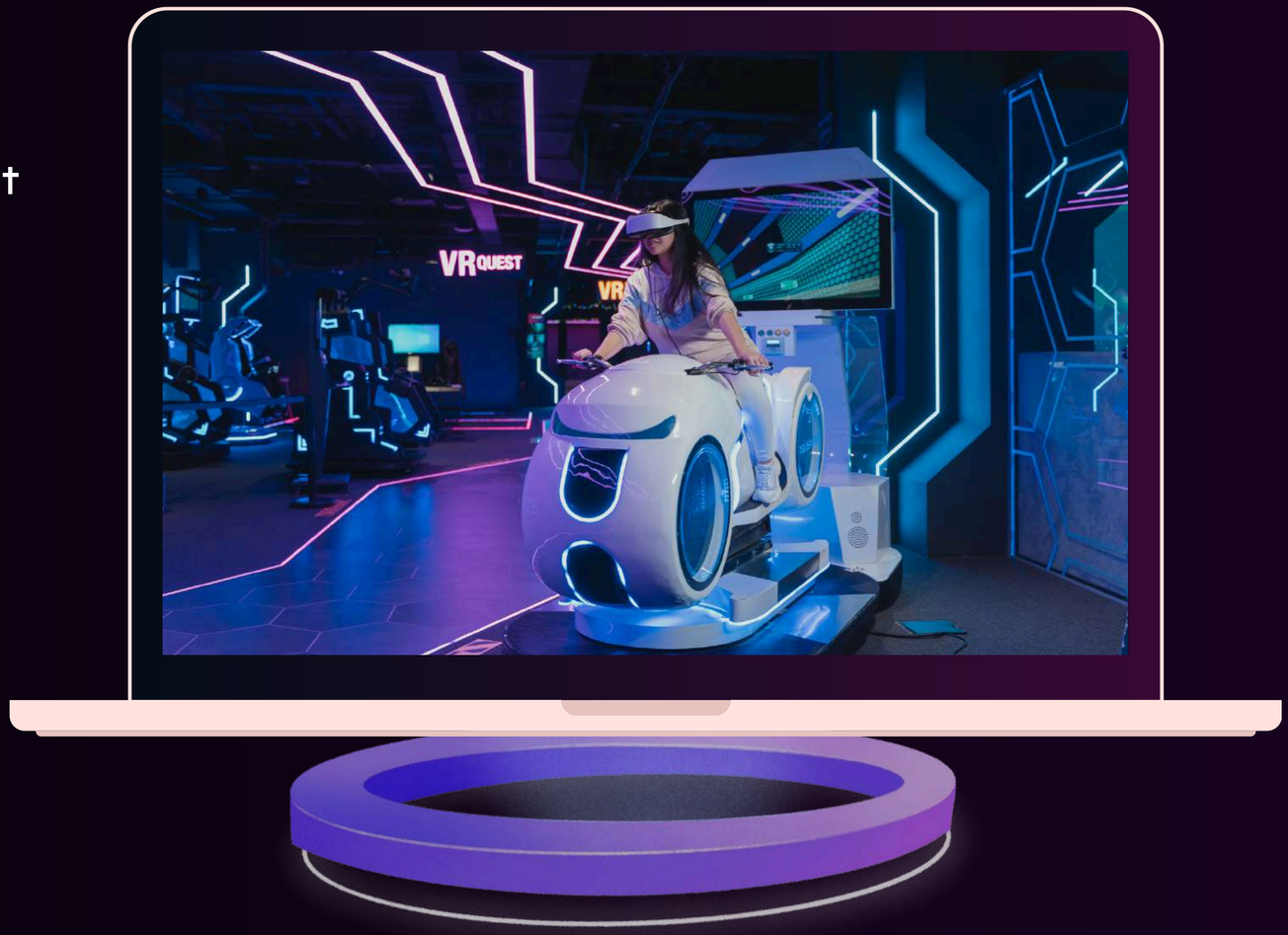
MACHINE LEARNING MODELS

We used Decision Tree and Random Forest algorithms.

Steps followed:

- Load and clean the dataset
- Train the model using labeled data (real/fake)
- Test the model on unseen data
- Evaluate using performance metrics

Random Forest gave better results than the Decision Tree.



RESULTS

- The model achieved an accuracy of around 90–92%
- We used accuracy, precision, and recall to measure performance
- Random Forest performed best in detecting fake accounts
- High recall ensured most fake accounts were caught
- Visualizations helped understand data patterns and model performance

CHALLENGES

Limited and Unbalanced Data

It was hard to find good datasets with real fake account data. Also, most datasets had more real accounts than fake ones, which made training the model tricky.

Realistic-Looking Fake Accounts

Some fake profiles were made to look very real, which confused the model and made it harder to spot them correctly.

Trial and Error in Feature Selection

Choosing the right features wasn't easy. We had to experiment multiple times to find the features that actually helped the model perform better.

FUTURE IMPROVEMENTS

Live Data Integration:
Connect the system to real platforms using APIs for real-time detection.

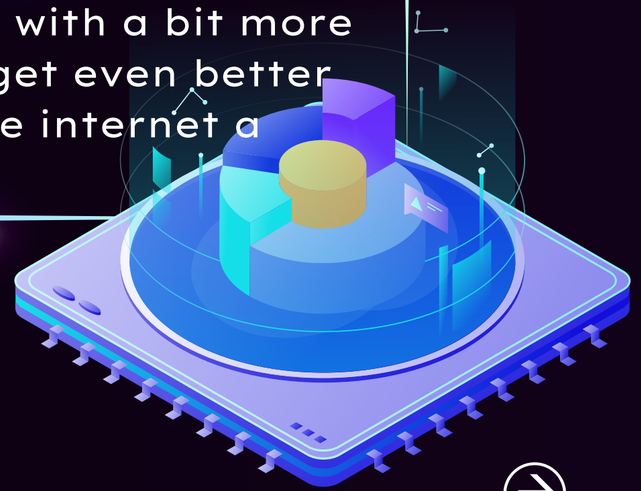
Smarter Models:
Use deep learning for better accuracy and to detect advanced fake accounts.

Content Analysis with NLP:
Analyze posts and messages to spot fake behavior through language patterns.

STUDIO
SHODWE

CONCLUSION

Through this project, we learned how fake accounts behave and how we can use machine learning to spot them. We looked at things like incomplete profiles, unusual activity, and follower patterns to train our model. Even though we faced some challenges—like not having enough real data—the results were really encouraging. Our system was able to catch most fake accounts, and with a bit more data and smarter tech, it can get even better in the future and help make the internet a safer place.



THANK YOU!