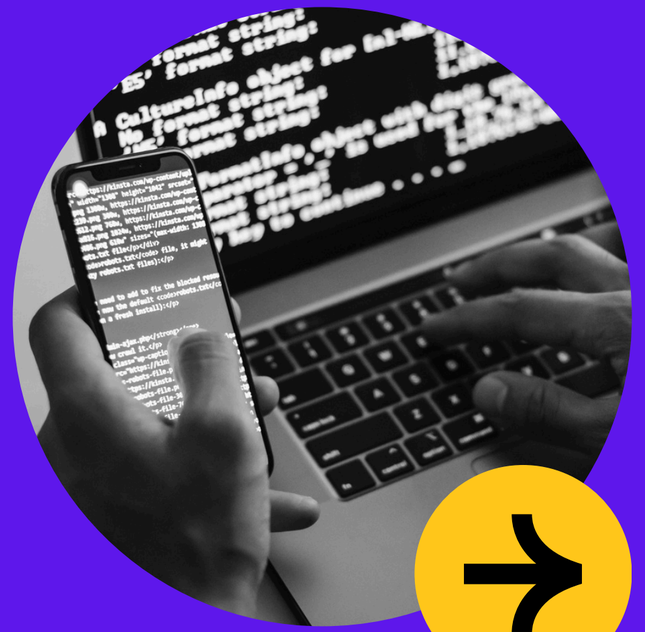
FAKE / PHISHING WEBSITE DETECTION

USING MACHINE LEARNING



BY : ANIL VHATKAR (A004)
OM PAWAR (A006)

INTRODUCTION

- In today's digital world, phishing attacks are one of the most common and dangerous forms of cybercrime.
- Phishing websites are designed to trick users into believing they are legitimate, often mimicking trusted websites to steal sensitive information such as login credentials, credit card details, and personal data.
- These attacks can result in significant financial losses, identity theft, and damage to reputation.

PROBLEM STATEMENT

As online transactions grow, phishing websites have become a major threat, tricking users into revealing sensitive information like passwords and financial data. This project aims to develop a machine learning model to detect phishing websites by analyzing features such as URL structure, website content, and domain information. The model will classify websites as legitimate or phishing

OBJECTIVES

01 Develop Machine Learning and Deep Learning Models

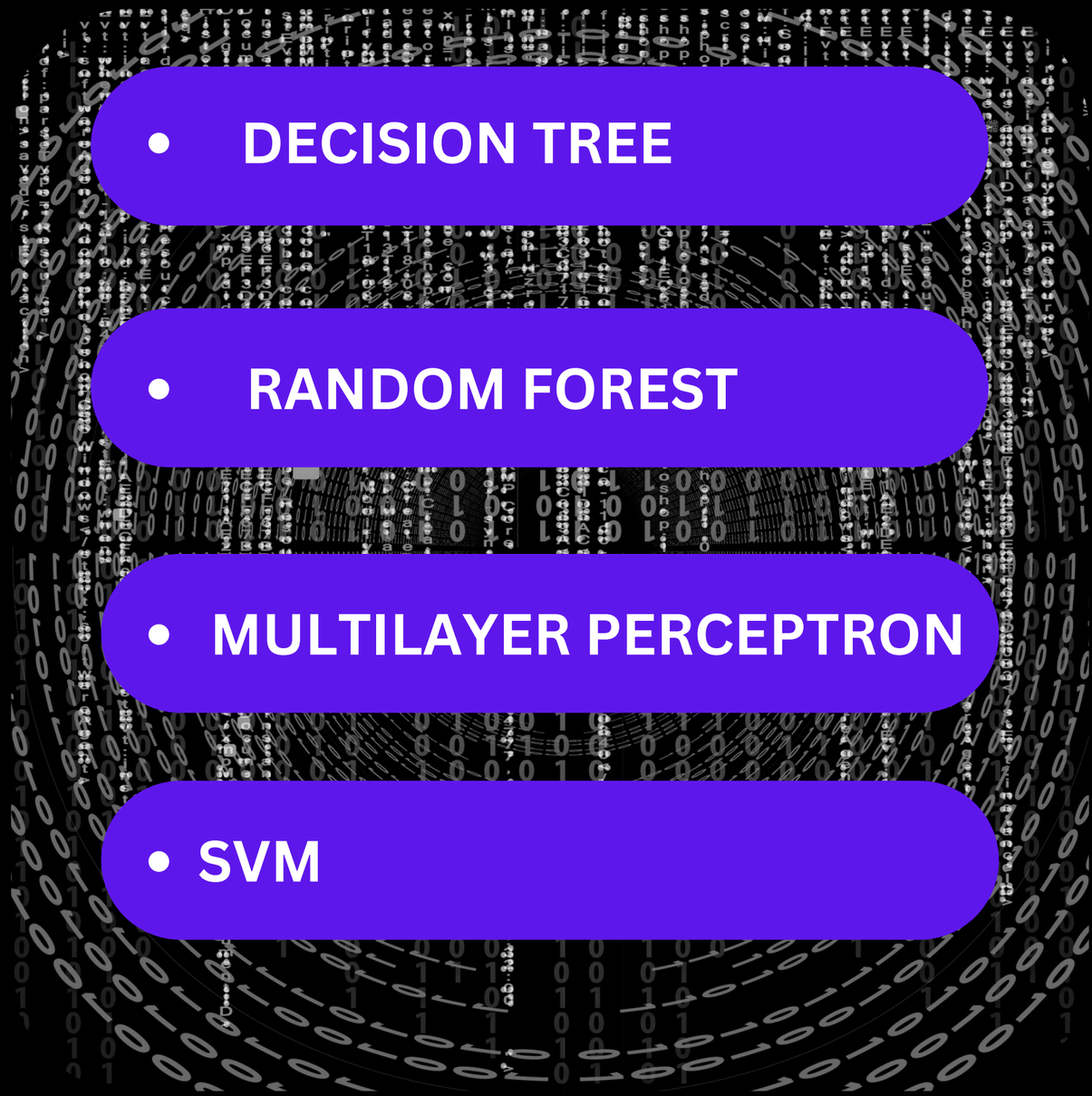
02 Automate Phishing Detection

03 Evaluate and Compare Model Performance

METHODOLOGY

For this project, Python was chosen for its versatility and rich libraries like Pandas, NumPy, and Scikit-learn, essential for data analysis and machine learning. Development was done in Google Colab, providing an interactive environment for code, documentation, and results. Pandas and NumPy facilitated efficient data loading, cleaning, and preprocessing of website features

MODELS USED



- DECISION TREE
- RANDOM FOREST
- MULTILAYER PERCEPTRON
- SVM

COLAB FILE LINK :

https://colab.research.google.com/drive/1jKHTkacBjbtz2CJnEoHPyj41aFH9n8Ee?usp=sharing

Conclusion and Next Steps

The phishing website detection model successfully distinguishes between phishing and legitimate sites. Multilayer Perceptron achieved the highest accuracy of 86% on the test data. The results demonstrate that machine learning can effectively automate phishing detection, reducing the risk of attacks

THANK YOU!