CYBERTHREAT ANALYSIS

Phishing email detection system

Submitted by: Adit Sharma
Mentor: Siddhant Thapliyal

Introduction

Phishing emails remain a persistent and costly cyber threat, tricking unsuspecting users into revealing sensitive information or downloading malware.

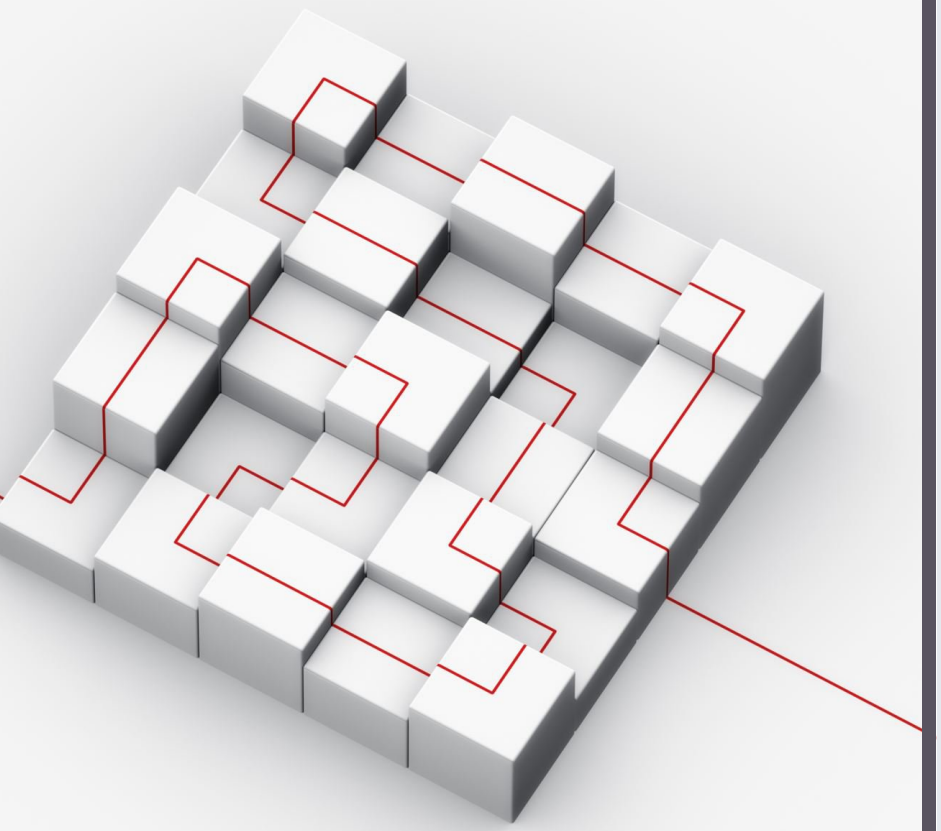
Our project tackles this issue by developing a system to automatically detect phishing emails, safeguarding individuals and organizations from these malicious attacks.

Objectives

Enhance Detection Accuracy: We aim to develop a robust system that surpasses existing detection methods in accurately identifying phishing emails.

Reduce User Reliance on Manual Detection: By creating an automated detection system, we aim to empower users and organizations to rely less on manual identification of phishing attempts.

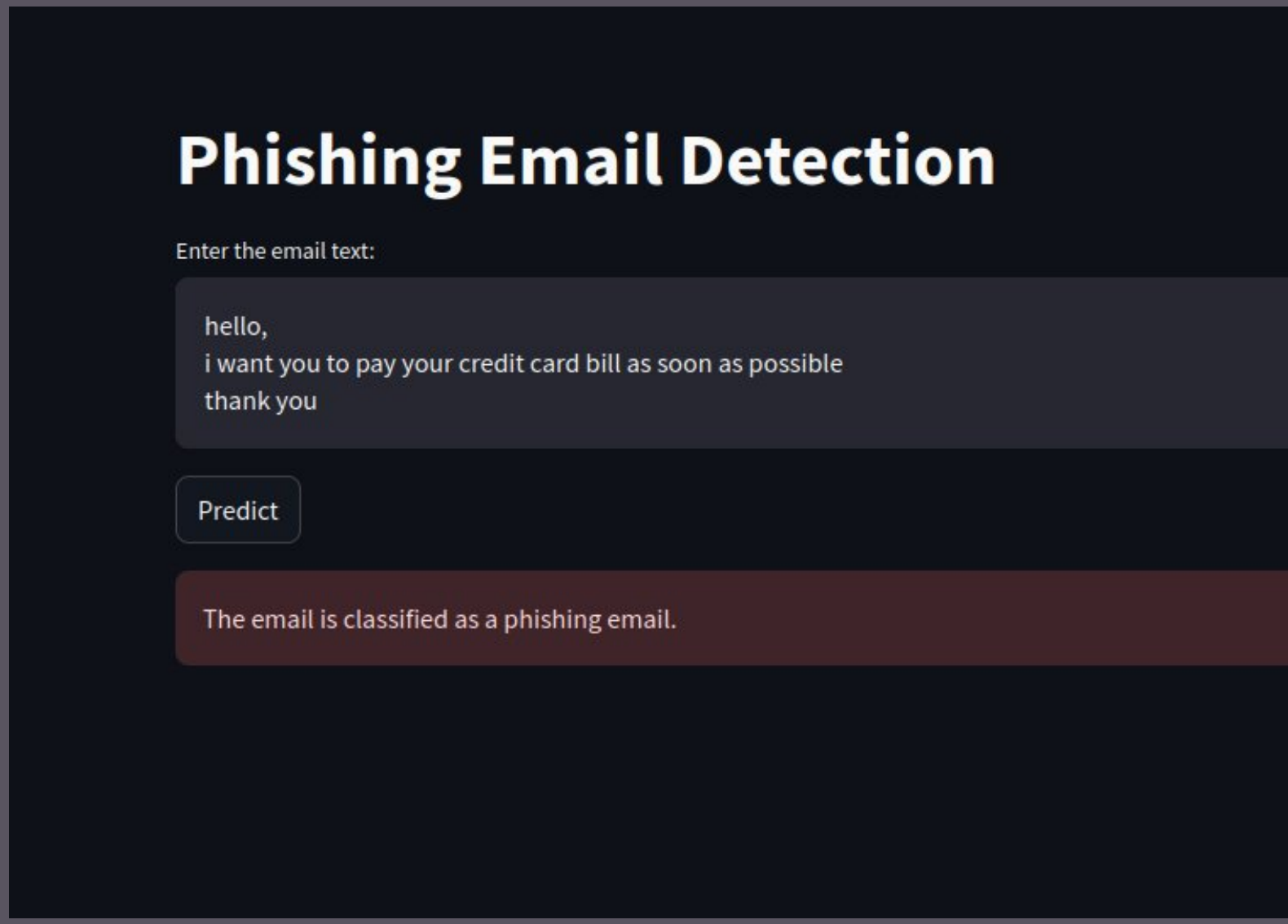
METHODOLOGY



1. **Data Preprocessing:** techniques like stemming and SMOTE have been used to pre-process the data and make it suitable for training the ML model.
2. **Training:** multiple models were trained on the chosen dataset and random forest model provided the highest accuracy of 97%
3. **User Interface:** streamlit, a python module was used to create interactive UI for easy access to the model. Users can easily input a mail and check whether it is safe or not.

Result

The Random Forest model trained on the dataset
of emails declared safe or classified as phishing provided a score of 97%



Future Work

- **Improved Dataset**: Enhance dataset diversity with more emails from various sources, languages, and time periods. Real-time data integration and detailed annotations can further enrich the dataset's quality.
- **Advanced Techniques**: Explore advanced machine learning approaches such as Recurrent Neural Networks (RNNs) and Transformer models (e.g., GPT) to capture complex email content dependencies and improve detection accuracy.
- **Enhanced Feature Extraction**: Utilize semantic analysis, behavioral features, and email metadata to extract deeper insights from email content and improve phishing detection capabilities.
- **Model Evaluation and Deployment**: Implement real-time evaluation, adaptive learning strategies, and user feedback integration to continuously refine and optimize the detection models in real-world environments.

THANK YOU