Member's

Punit Gavali
9712

Janet Nelson
9717

Sheldon Chettiar
9697

Akshat Sarraf
9742


AI-enabled Phishing Links Detection
and Alert System chrome extension

Problem Statement

Develop an AI-enabled phishing link detection chrome extension using machine learning that can accurately identify and classify phishing links in real-time. The system should be able to analyze various features of a link, such as URL structure, domain reputation, and content, to determine the likelihood of it being a phishing link.

Increasing Phishing Attacks

Phishing attacks are becoming more sophisticated, making it challenging to detect malicious links.

User Vulnerability

Users often struggle to identify phishing links, leading to potential security breaches.

Time-consuming Manual Checks

Manually verifying every link is time-consuming and impractical for users.

Abstract

This research proposal aims to develop an advanced phishing detection solution using machine learning algorithms and real-time analysis across various platforms. The solution will enhance detection accuracy by analyzing content, behavior, email, social media, and instant messenger app content, and provide phishing source identification for appropriate response actions.

Objective

The main objective of an AI-enabled Phishing Links Detection and Alert System is to proactively identify and alert users or organizations to potential phishing threats, safeguarding sensitive data and promoting cybersecurity awareness. It accomplishes this by employing machine learning algorithms to detect phishing attempts in real-time, verify the legitimacy of web links, analyze email content, and provide adaptive protection while integrating seamlessly with existing communication channels.

KEY FEATURES AND FUNCTIONALITY OF THE CHROME EXTENSION

Real-Time Link Analysis

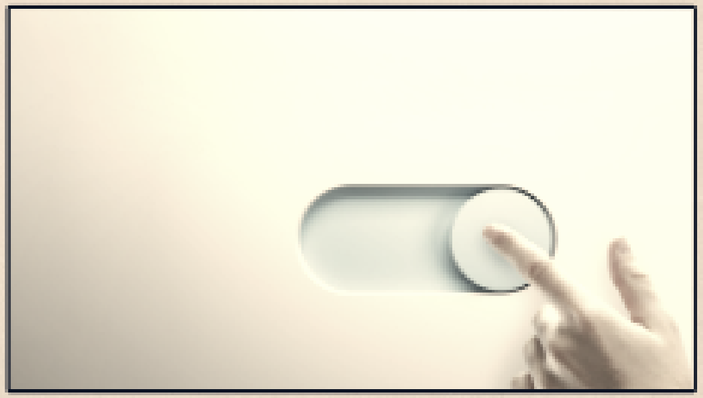
The extension analyzes links in real-time, leveraging AI algorithms to detect phishing attempts.

Browser Integration

Seamlessly integrates with popular web browsers, providing users with constant protection.

User-Friendly Interface

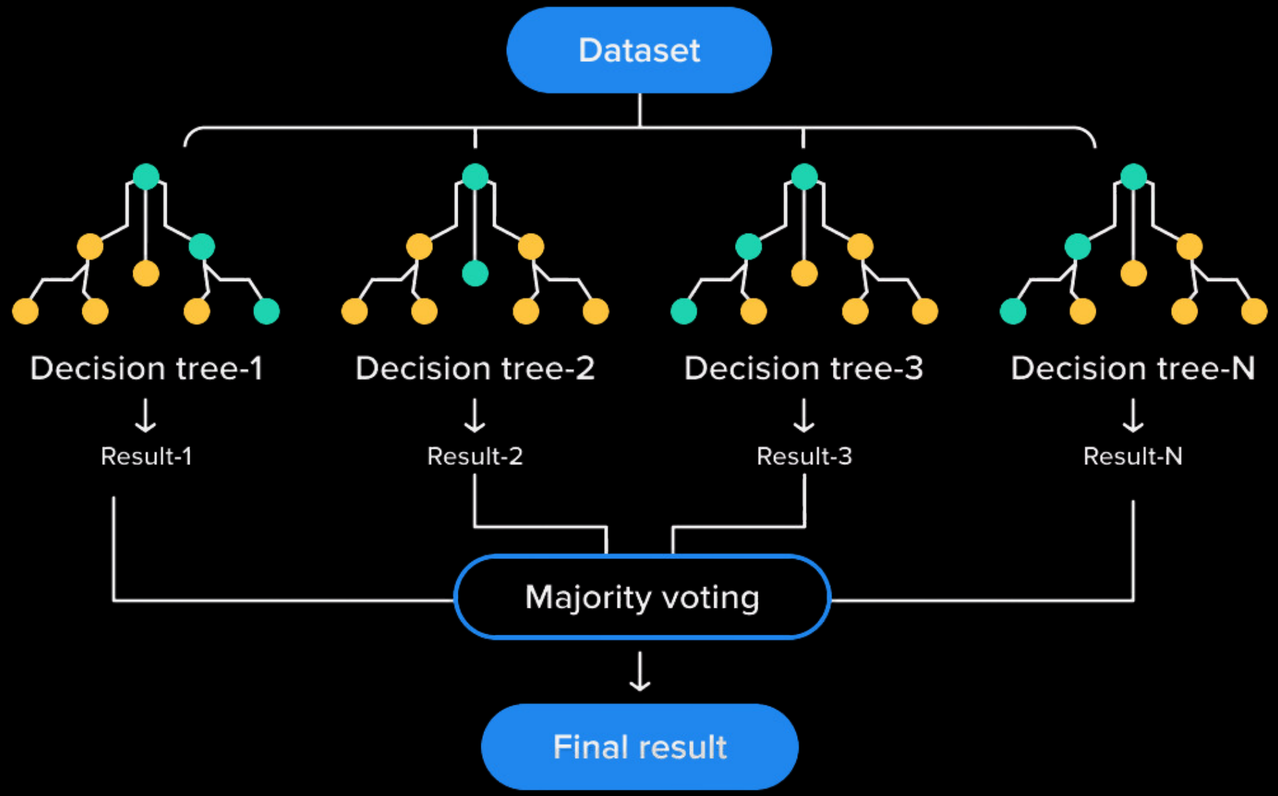
The extension offers an intuitive interface, making it easy for users to understand and interact with.



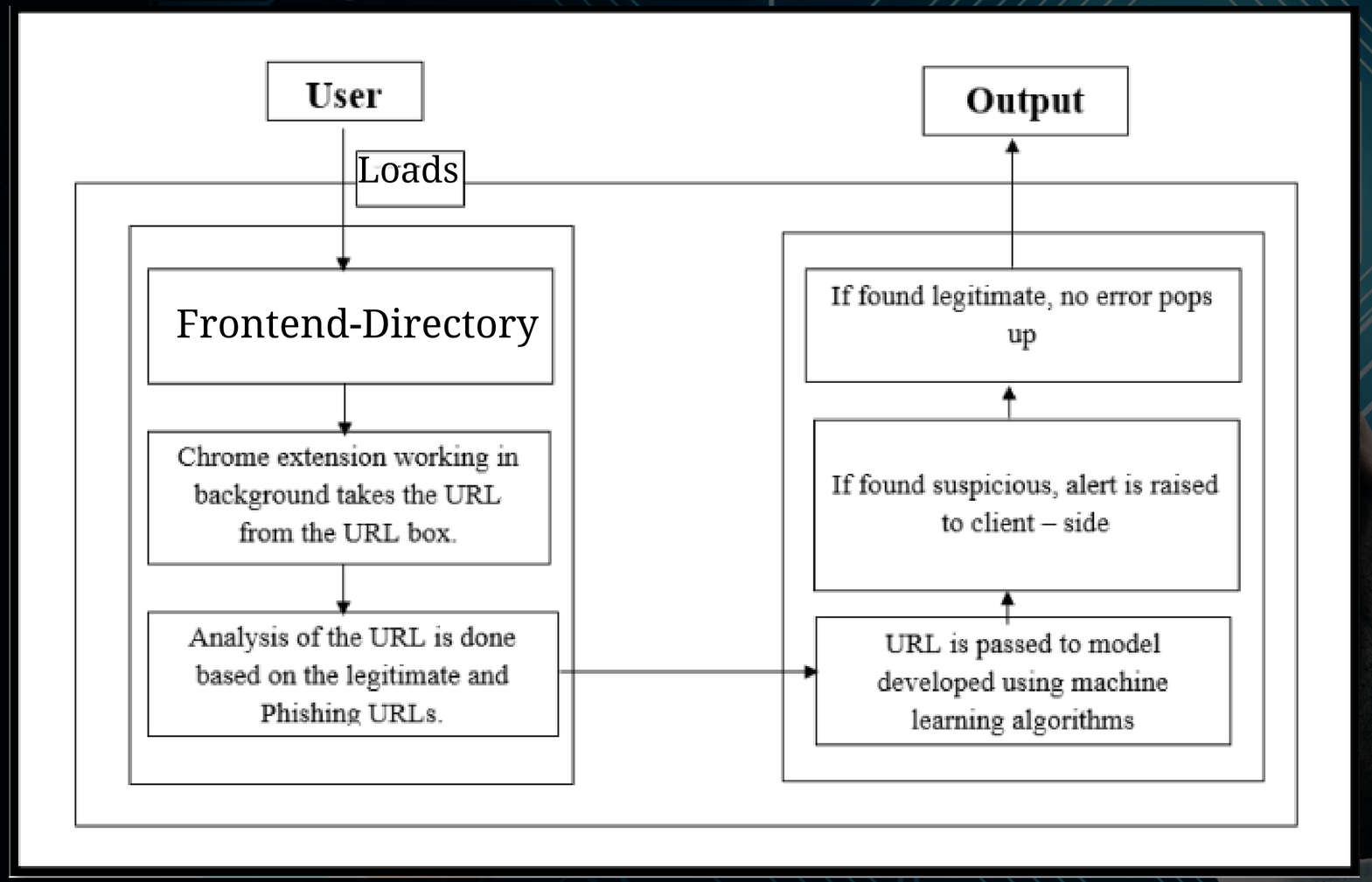
Overall requirements

Machine learning algorithm

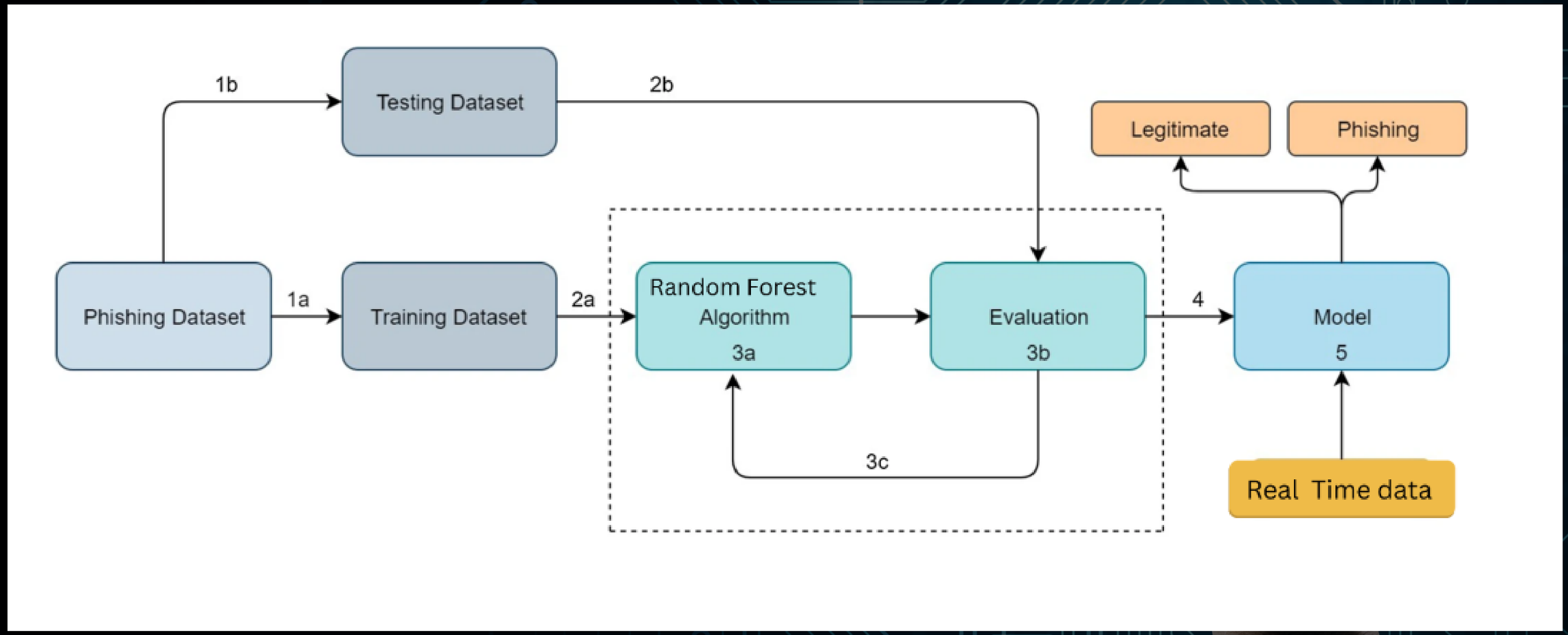
Random Forest is a machine learning algorithm technique that is utilized for both classification and regression tasks. It is an ensemble method that chains multiple decision trees to make predictions.



Basic Model :- How it works



Block Diagram

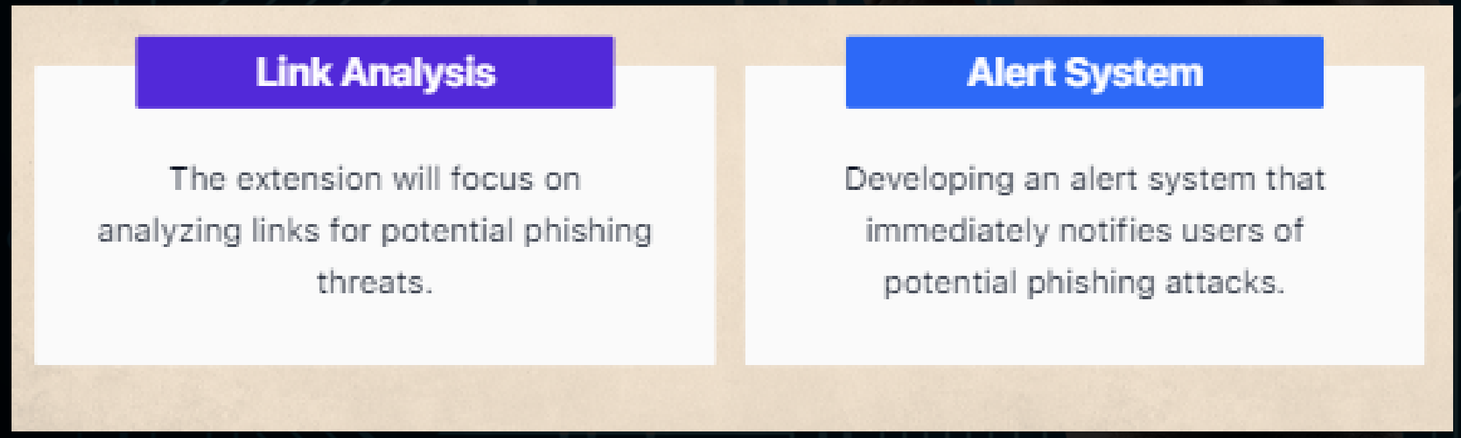


Applications and Social Relevance

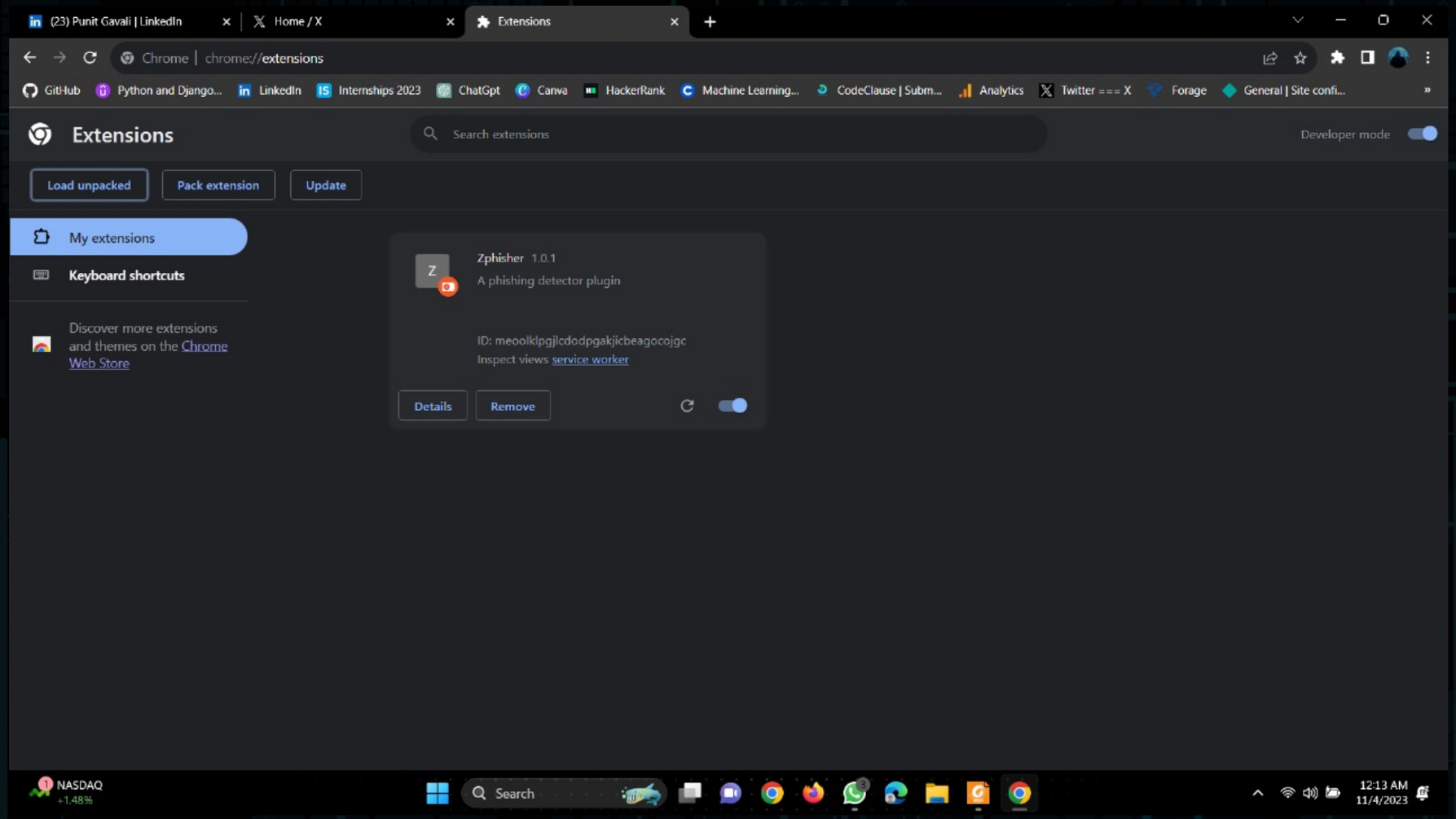
- Personal cybersecurity
- Corporate cybersecurity
- Financial institutions
- Government and public sector
- Social media platforms
- Overall online security

Scope of Project

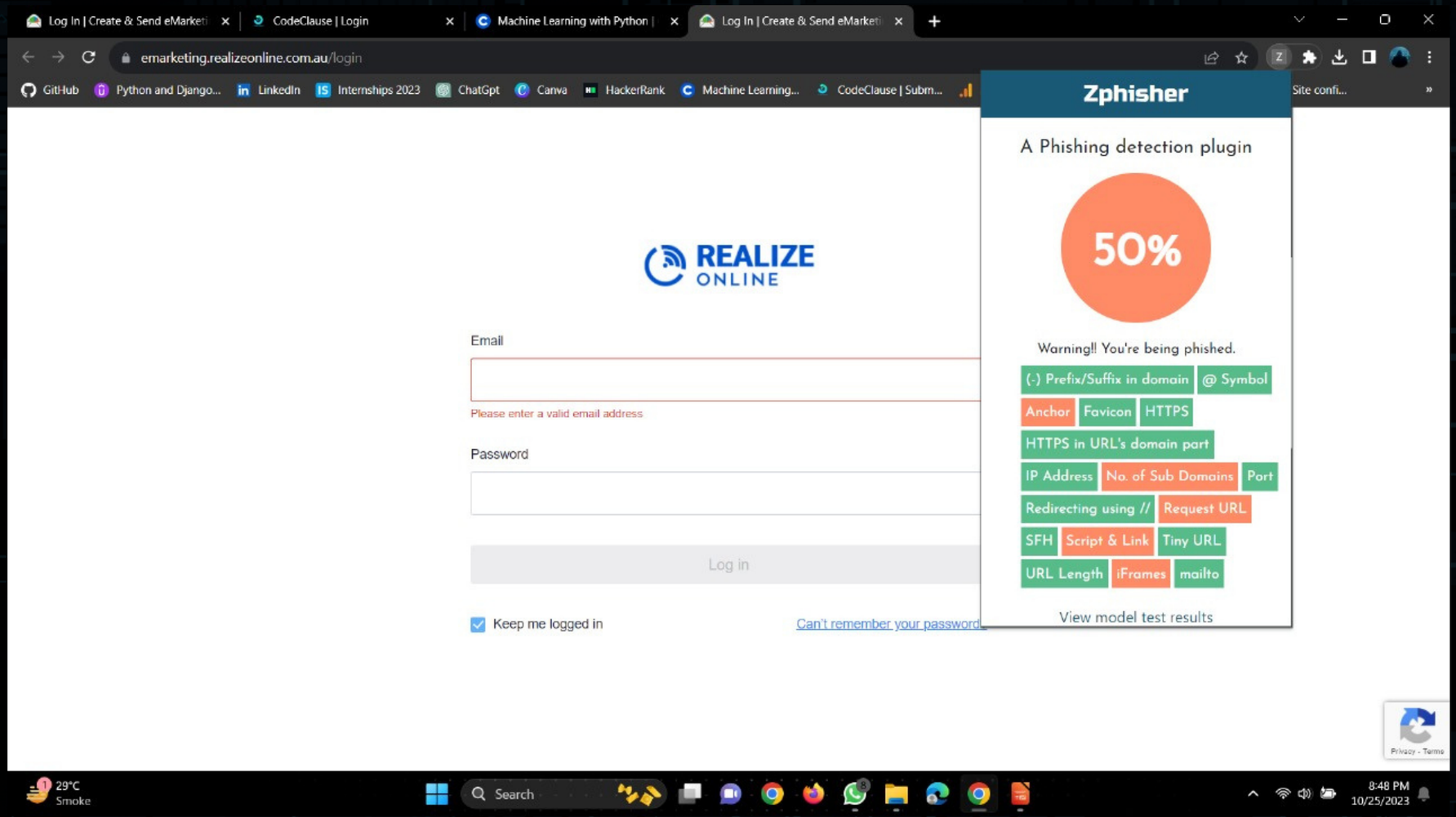
This project centers on creating an AI-powered system for phishing link detection using machine learning models trained on diverse datasets. It involves real-time monitoring and alerting to bolster online security while incorporating user feedback for ongoing refinement. The overarching objective is to proactively identify and counter phishing threats in digital landscapes, enhancing cybersecurity.



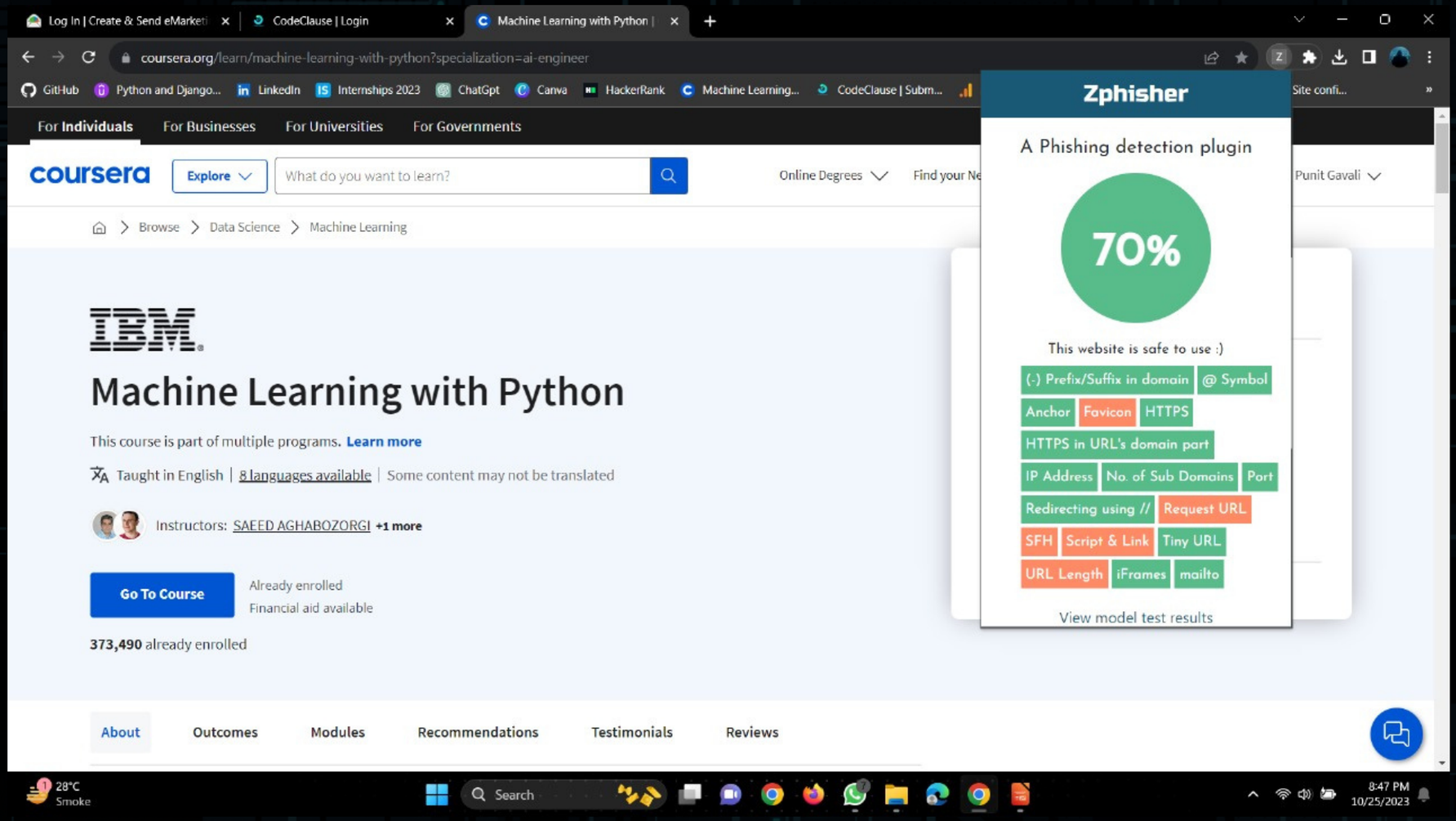
LOADING OF EXTENSION



IMPLEMENTATION



IMPLEMENTATION



Conclusion

This chrome extension AI-enabled Phishing Links Detection and Alert Systems consistently conclude that machine learning and deep learning techniques are highly effective in identifying malicious URLs. Feature engineering, real-time monitoring, and ensemble models play critical roles in improving detection accuracy. Dynamic behavioral analysis, addressing data imbalance, and adapting to evolving phishing tactics are key challenges and areas of research.

Reference

"A Survey of Phishing Detection and Defense Techniques" by Alsaleh et al. (2019.

- "A novel phishing webpage detection approach with convolutional neural networks" by Fouladi et al. (2018).
- https://link.springer.com/article/10.1007/s11235-020-00733-2
- https://towardsdatascience.com/phishing-domain-detection-with-ml-5be9c99293e5
- https://arxiv.org/pdf/2201.10752
- https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0258361

Thank You