



# Member's



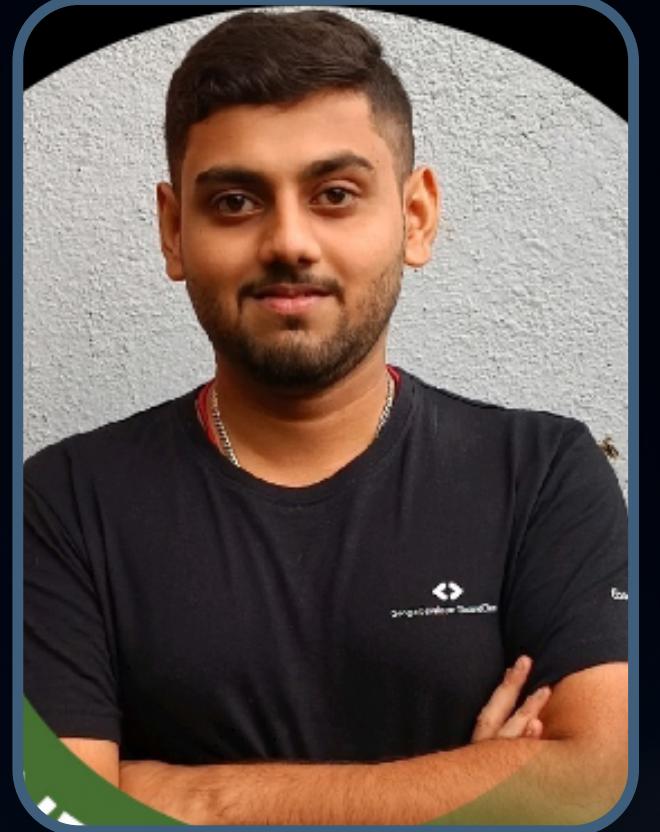
Punit Gavali  
9712



Janet Nelson  
9717



Sheldon Chettiar  
9697



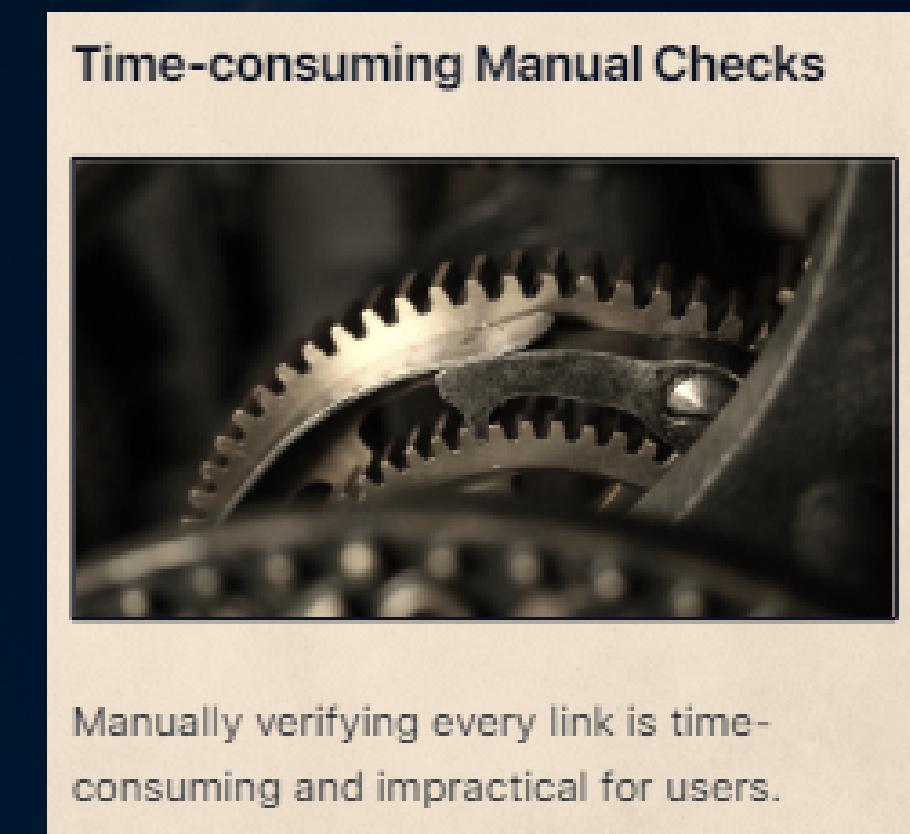
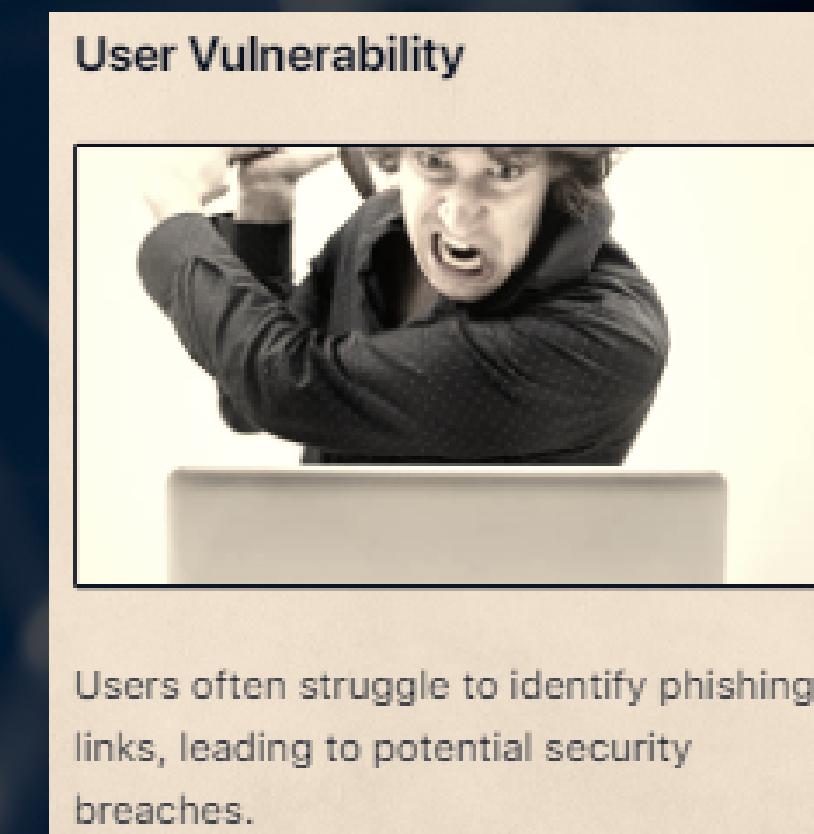
Akshat Sarraf  
9742



# 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.**



# 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.

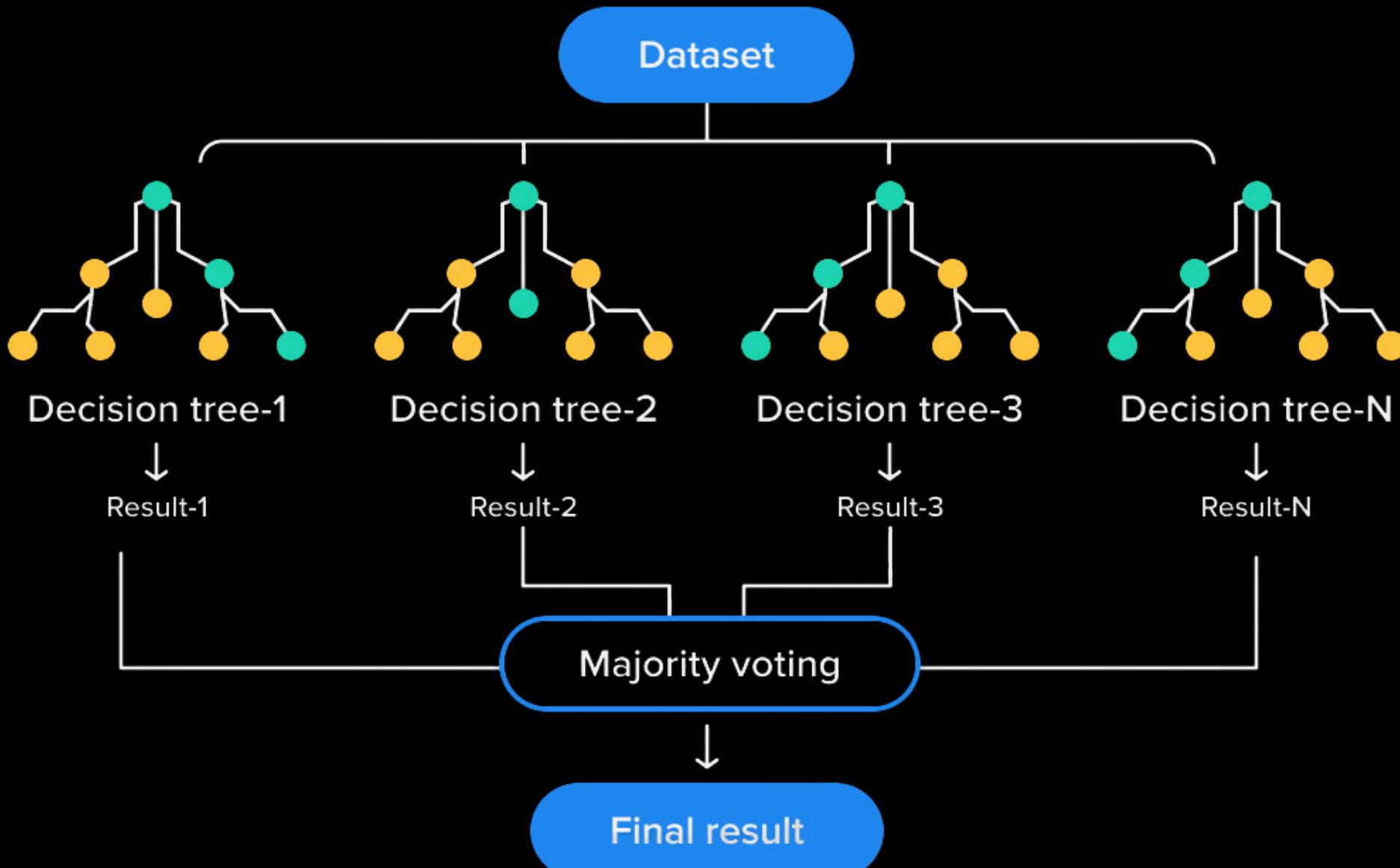


# Overall requirements

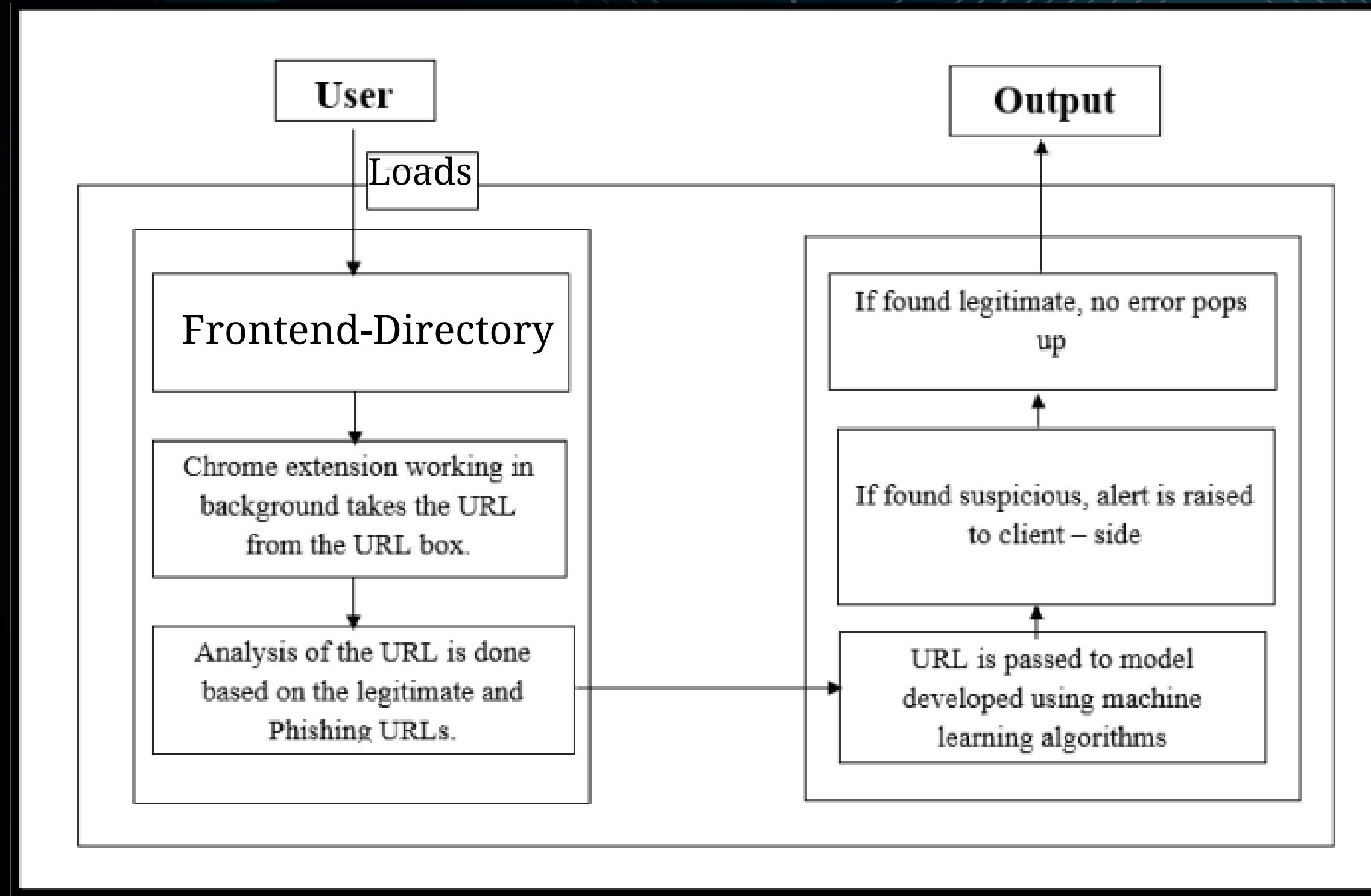


# Machine learning algorithm

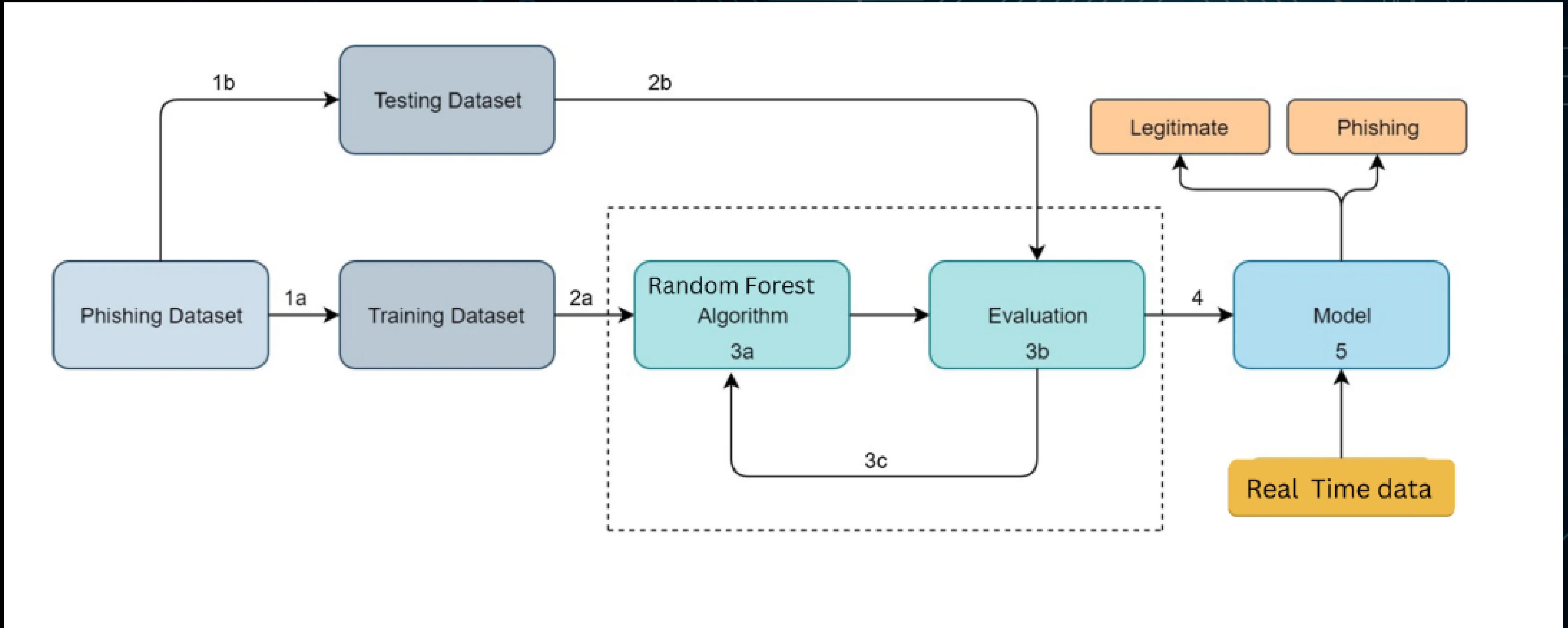
**Random Forest is a machine learning algorithm technique that is utilized for both classification and regression tasks. It is an ensemble method that chains multiple decision trees to make predictions.**



# 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.

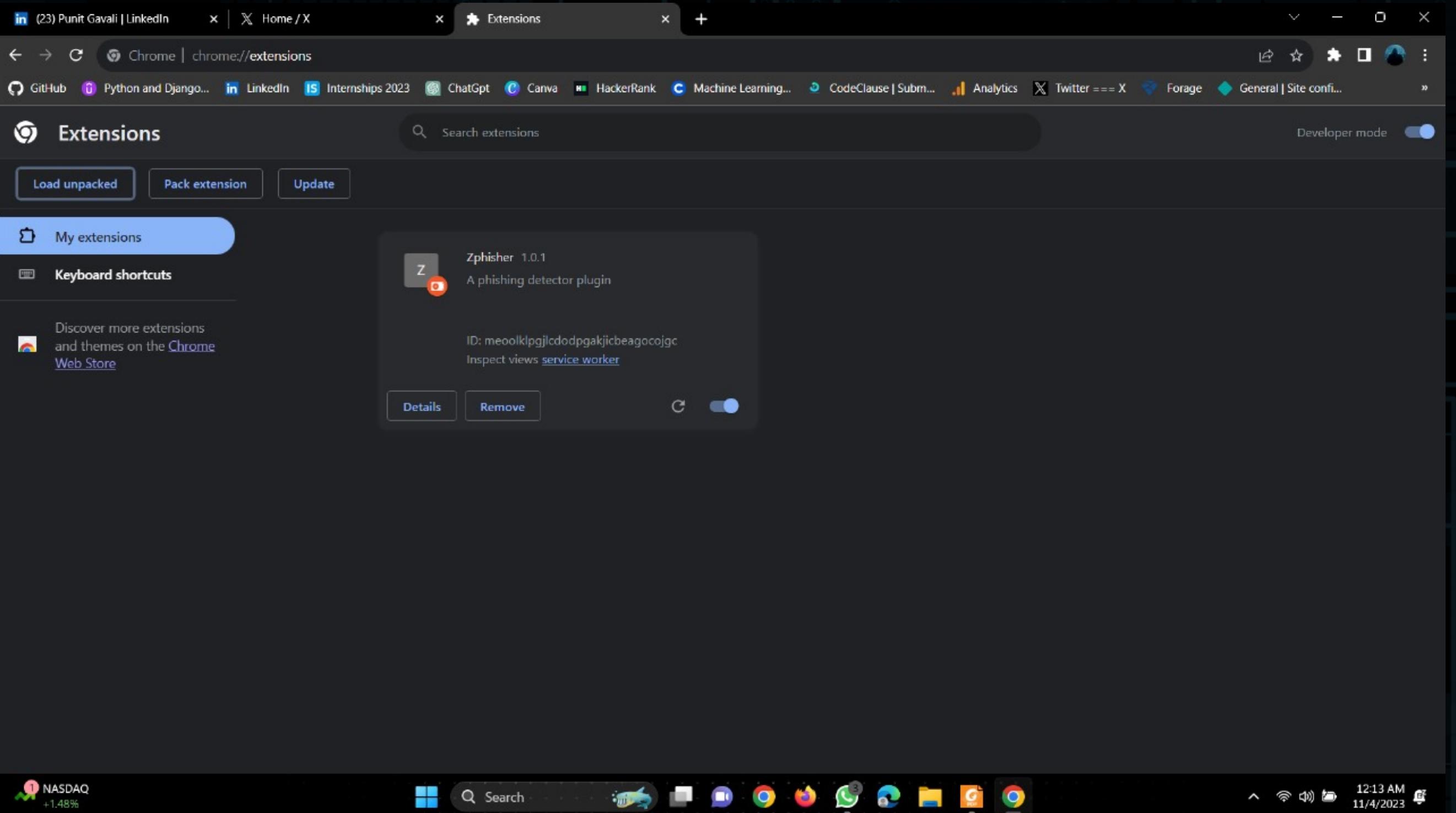
## Link Analysis

The extension will focus on analyzing links for potential phishing threats.

## Alert System

Developing an alert system that immediately notifies users of potential phishing attacks.

# LOADING OF EXTENSION



# IMPLEMENTATION

The image shows a web browser window with multiple tabs open. The active tab is for 'emarketing.realizeonline.com.au/login'. The page displays a 'REALIZE ONLINE' logo and a login form with fields for 'Email' and 'Password'. A large orange circle on the right side of the screen contains the text '50%'.

**Zphisher**  
A Phishing detection plugin

Warning!! You're being phished.

(-) Prefix/Suffix in domain @ Symbol  
Anchor Favicon HTTPS  
HTTPS in URL's domain part  
IP Address No. of Sub Domains Port  
Redirecting using // Request URL  
SFH Script & Link Tiny URL  
URL Length iFrames mailto

View model test results

At the bottom of the screen, there is a taskbar with various icons and a system tray showing the date and time.

# IMPLEMENTATION

The screenshot shows a web browser window with three tabs open:

- Log In | Create & Send eMarketin...
- CodeClause | Login
- Machine Learning with Python | coursera.org

The main content area displays the Coursera course page for "Machine Learning with Python" by IBM. The page includes:

- The IBM logo.
- The title "Machine Learning with Python".
- A note stating "This course is part of multiple programs. [Learn more](#)".
- A language availability section: "Taught in English | [8 languages available](#) | Some content may not be translated".
- Instructor information: "Instructors: SAEED AGHABOZORGI +1 more".
- A blue "Go To Course" button.
- Enrollment statistics: "Already enrolled" and "Financial aid available".
- A total enrollment count of "373,490 already enrolled".
- Navigation links: About, Outcomes, Modules, Recommendations, Testimonials, Reviews.
- A weather widget showing "28°C Smoke".
- A system tray at the bottom right showing icons for search, file explorer, and other applications.

A modal window titled "Zphisher" is overlaid on the page, indicating a "Phishing detection plugin". It shows a large green circle with "70%" and the text "This website is safe to use :)". Below this, it lists various security metrics with colored status indicators:

- (-) Prefix/Suffix in domain @ Symbol
- Anchor Favicon HTTPS
- HTTPS in URL's domain part
- IP Address No. of Sub Domains Port
- Redirecting using // Request URL
- SFH Script & Link Tiny URL
- URL Length iFrames mailto

At the bottom of the modal, there is a link "View model test results".

# 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*

