# Phishing

- Narwhal Sentinels

# Basic Understanding

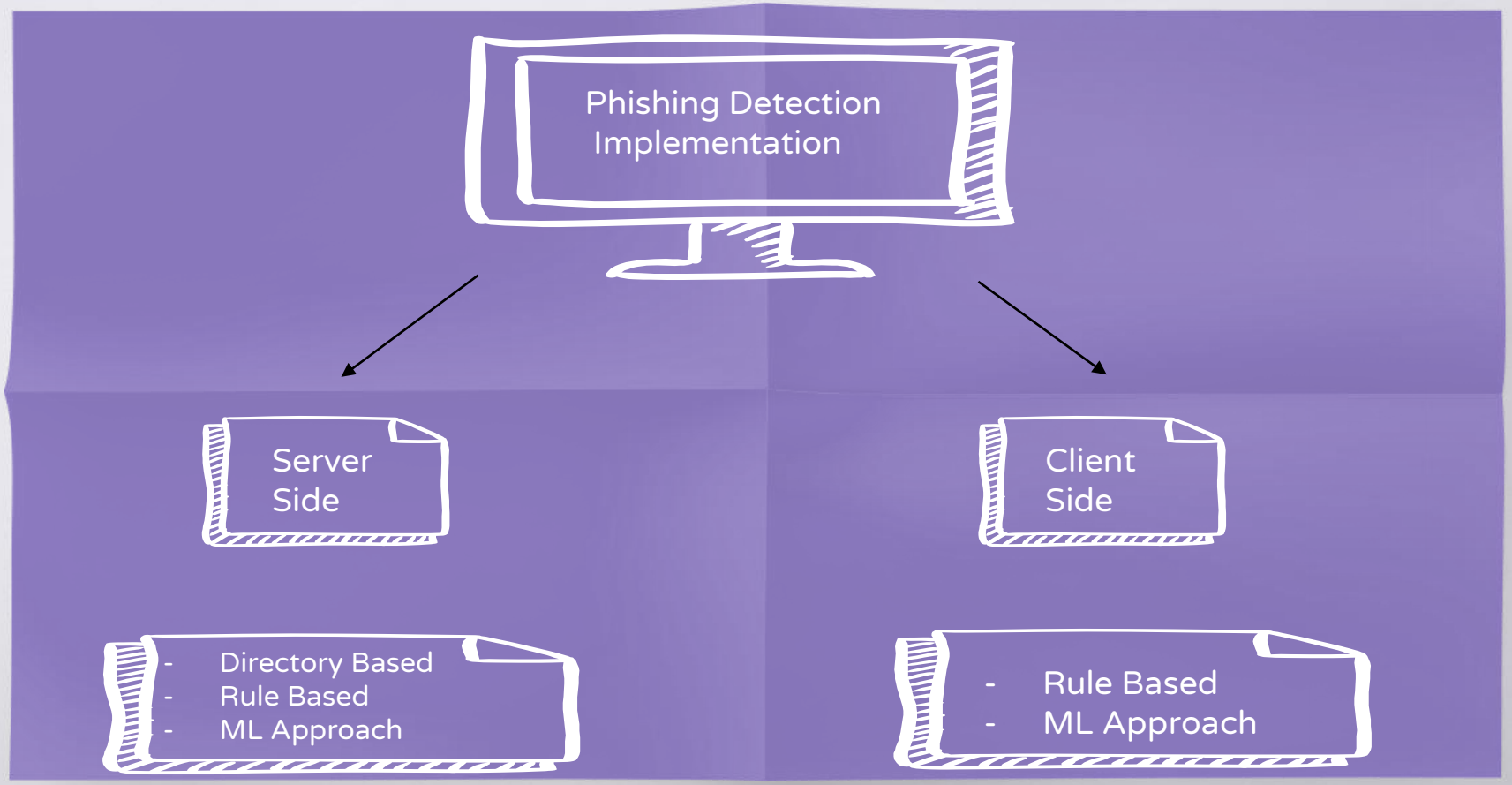
- **Phishing** is the fraudulent attempt to obtain **sensitive information** such as usernames, passwords, and credit card details, often for **malicious reason**.
- It is typically carried out by **email spoofing** and it often directs users to enter personal information at a fake website, the looks of which are **identical to the legitimate site**, only differs in the URL.

# WORKS THAT ARE SIMILAR

1. A. Ahmed and N. A. Abdullah, "Real time detection of phishing websites," 2016 IEEE7th Annual Information Technology, Electronics and Mobile CommunicationConference (IEMCON), 2016.

2. Web Phishing Detection Using a Deep Learning Framework (2018)Authors : Ping Yi, Yuxiang Guan, Futai Zou, Yao Yao, Wei Wang, and Ting Zhu

3. Detection of phishing websites using an efficient feature-based machine learning framework (2018)Authors : Routhu Srinivasa Rao, Alwyn Roshan Pais


Phishing Detection Implementation
Server Side
Client Side
- Directory Based
- Rule Based
- ML Approach
- Rule Based
- ML Approach

# Proposed System

A Browser plugin that aims to detect phishing websites and warn the user.

## ML BASED APPROACH

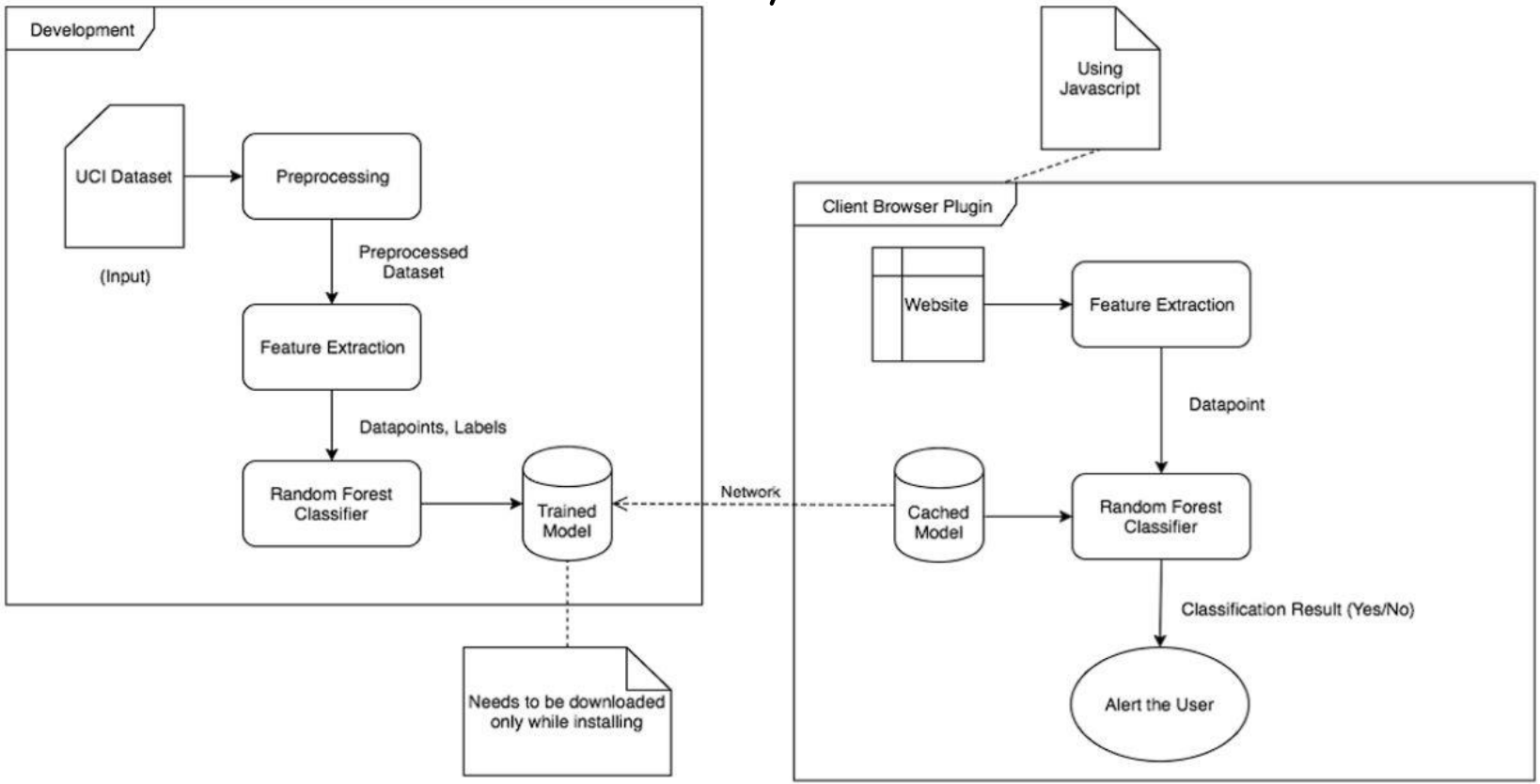
Real time detection of phishing websites discusses an approach based on features from only the URL of the website.

They were able to come up with a detection mechanism that is capable of detecting various types of phishing attacks maintaining a low rate of false alarms.

## DRAWBACKS

- The main disadvantage is that rule based methods are usually not the best performers in terms of prediction quality. Other methods (Forests, SVM, deep-nets) tends to be better.

# System Architecture



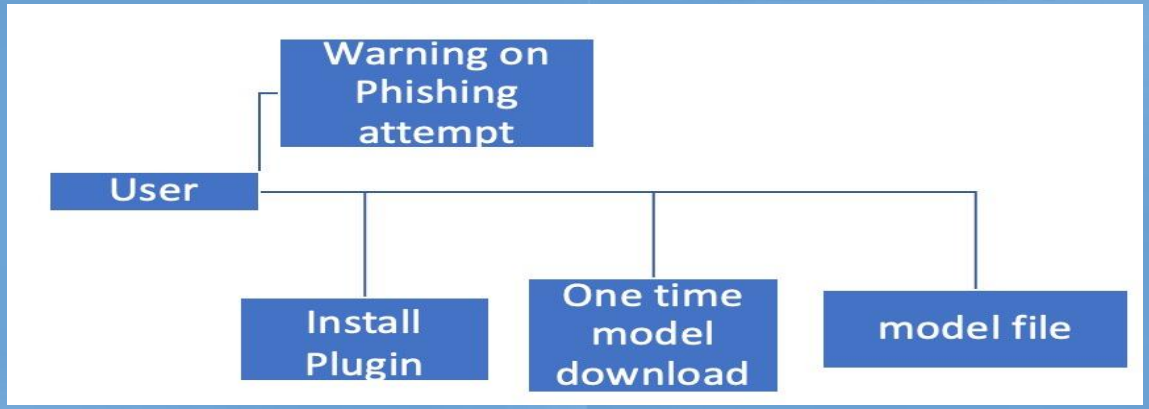
# USE CASE DIAGRAM

Pre condition -

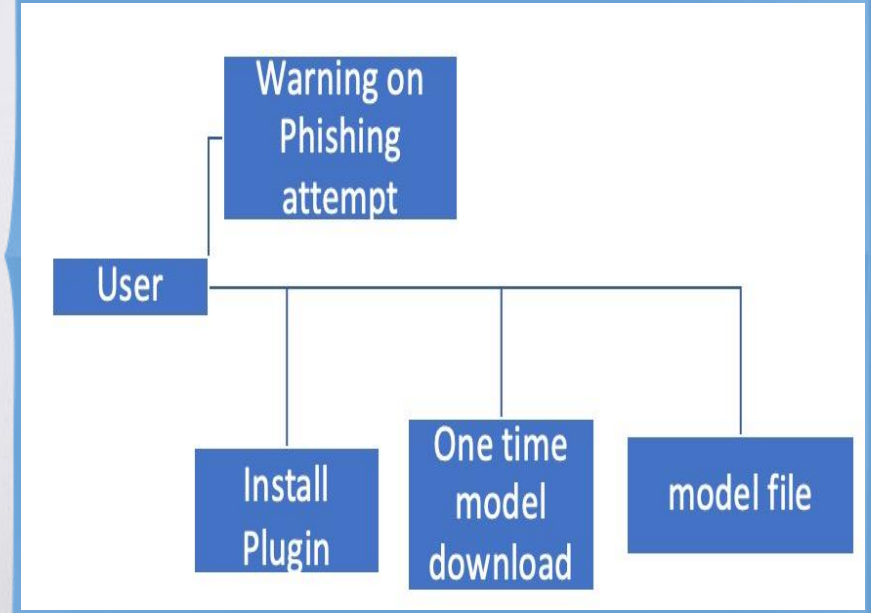
The user visits a website and have plugin installed.

Post condition -

The user is warned in-case it is a phishing website.



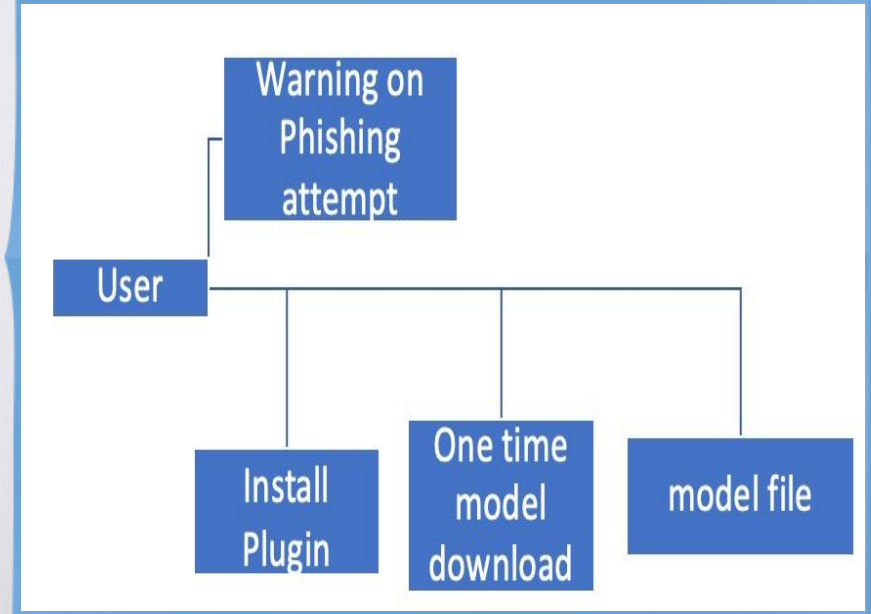
# USE CASE DIAGRAM




The overall use case diagram of the entire system is shown in the figure.

The user can install the plugin and then can continue his normal browsing behaviour.

# USE CASE DIAGRAM

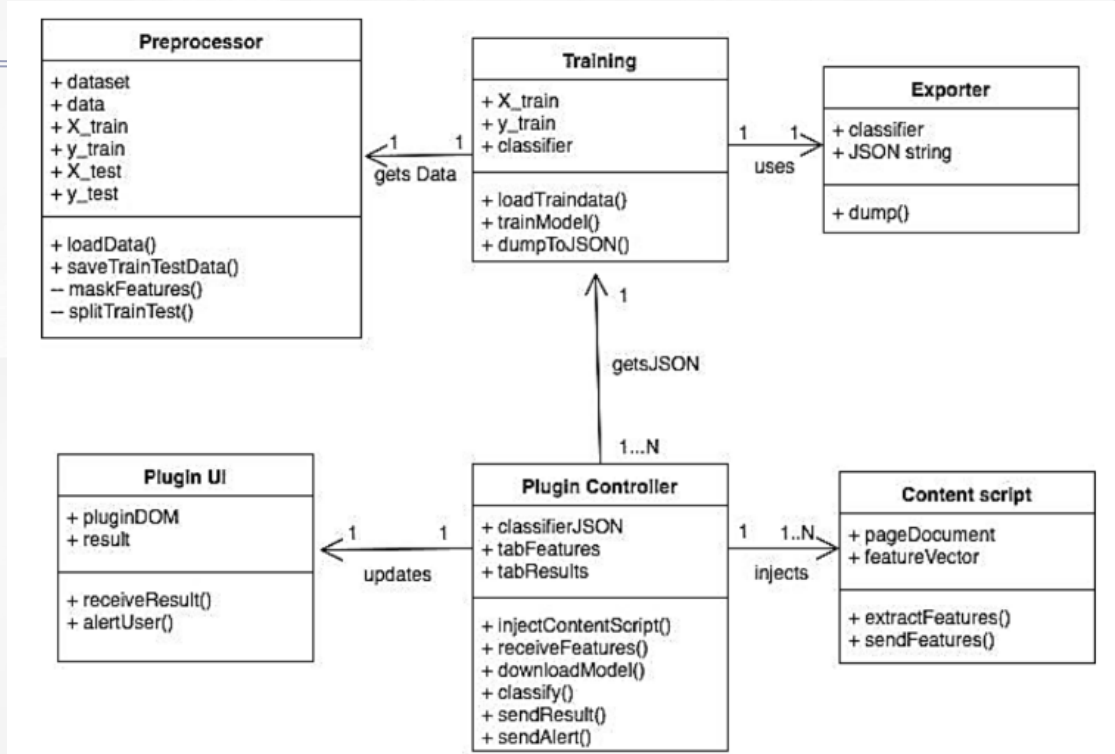



He only needs to download the model once.

This plugin will automatically check the browsing pages for phishing and warns the user for the same.

# Class Diagram

This diagram depicts the functions of various modules in the system clearly.



# TRAINING

- **INPUT** : *Training and testing data npy format.*

- **OUTPUT**: *Trained random forest classifier model.*

# TRAINING

## ▧ Pseudocode:

- Start
- Load training set from file calculate cross validation score.
- Train random forest classifier load testing set from file
- Calculate F1 score on testing set.
- End

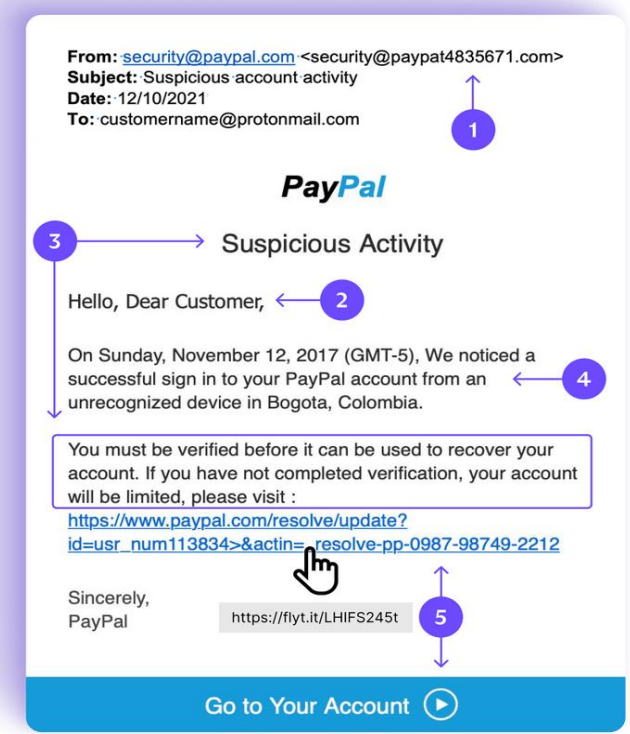
# PLUGIN

- INPUT : *Website viewed by the user.*

- OUTPUT: *Alert/Popup to the user.*

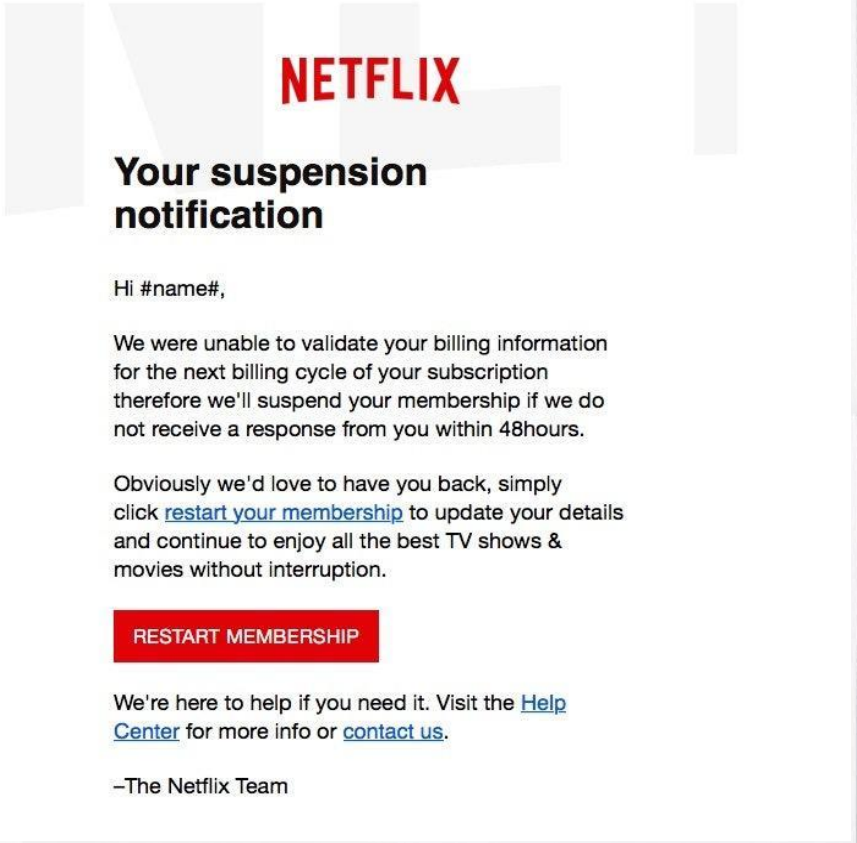
# Examples

Victim was attempted to get phished by faking the paypal order.



Victim was attempted to get phished by faking the netflix order.

The hacker used urgency inorder to easily phish the victim.



NETFLIX

**Your suspension notification**

Hi #name#,

We were unable to validate your billing information for the next billing cycle of your subscription therefore we'll suspend your membership if we do not receive a response from you within 48hours.

Obviously we'd love to have you back, simply click restart your membership to update your details and continue to enjoy all the best TV shows & movies without interruption.

RESTART MEMBERSHIP

We're here to help if you need it. Visit the Help Center for more info or contact us.

–The Netflix Team

## THE TEAM BEHIND THE PRODUCT