README

DATE	28-10-2022
PROJECT NAME	WEB PHISHING DETECTION
TEAM ID	PNT2022TMID28852
TEAM MEMBERS	1. SWARNA RAJINI 2. B.ANANTHA KUMAR 3. C.H.GIREESH BABU 4. D.SANTHOSH
MARKS	4 MARKS

WEB PHISHING DETECTION

IBM-PROJECT-51643-1660981142

BATCH NAME:B1-1M3E

TEAM ID-PNT2033TMID28852

TEAM MEMBERS:

1. SWARNA RAJINI
2. B.ANANTHA KUMAR
3. CH.GIREESH BABU
4. D.SANTHOSH

PROJECT OBJECTIVES:

BY THE END OF THE PROJECT:

- We'll be able to understand the problem to classify if it is a regression or a classification kind of problem.
- We will be able to know how to pre-process/clean the data using different data pre-processing techniques.
- Applying different algorithms according to the dataset
- We will be able to know how to find the accuracy of the model.
- We will be able to build web applications using the Flask framework.

INTRODUCTION:

There are a number of users who purchase products online and make payments through e-banking. There are e-banking websites that ask users to provide sensitive data such as username, password & credit card details, etc., often for malicious reasons. This type of e-banking website is known as a phishing website. Web service is one of the key communications software services for the Internet. Web phishing is one of many security threats to web services on the Internet.

Common threats of web phishing :

1. Web phishing aims to steal private information, such as usernames, passwords, and credit card details, by way of impersonating a legitimate entity.

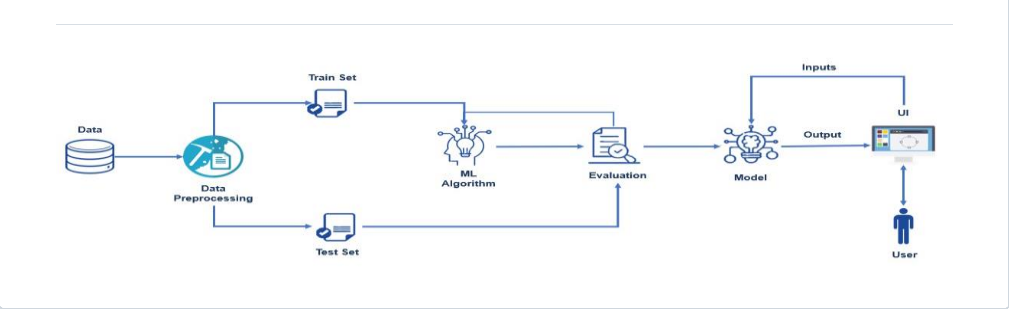
2. It will lead to information disclosure and property damage.

3. Large organizations may get trapped in different kinds of scams.

4. This Guided Project mainly focuses on applying a machine-learning algorithm to detect Phishing websites.

In order to detect and predict e-banking phishing websites, we proposed an intelligent, flexible and effective system that is based on using classification algorithms. We implemented classification algorithms and techniques to extract the phishing datasets criteria to classify their legitimacy. The e-banking phishing website can be detected based on some important characteristics like URL and domain identity, and security and encryption criteria in the final phishing detection rate. Once a user makes a transaction online when he makes payment through an e-banking website our system will use a data mining algorithm to detect whether the e-banking website is a phishing website or not.

TECHNICAL ARCHITECTURE:


Data
Data Preprocessing
Train Set
Test Set
ML Algorithm
Evaluation
Model
Inputs
Output
UI
User