PROJECT DESIGN PHASE-I

PROPOSED SOLUTION TEMPLATE

TEAM ID - PNT2022TMID21307

PROJECT NAME- Web Phishing Detection

TEAM MEMBERS:

VARSHINI S - 917719C111

RUCHITAA RAJ N R- 917719C083

RAMPRASAD R - 917719C078

DEEPAK RM - 917719C014

PROBLEM STATEMENT:

Numerous users 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.

IDEA / SOLUTION DESCRIPTION:

The main objective of the project is applying a machine-learning algorithm to detect Phishing websites. It is a web application to detect good and malicious URLs i.e web phishing sites. We employ HTML, CSS, and JavaScript for the website and the web application is deployed using Flask framework. Different ML models are run and the one with the high accuracy will be selected for final model. The dataset is downloaded and then run on notebooks. Necessary preprocessing techniques are implemented by applying various statistical methods and encodings are done. Then it is split to train test model and different algorithms are tried.

UNIQUENESS/NOVELTY:

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 like logistic regression,SVM,KNN 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.

SOCIAL IMPACT/ CUSTOMER SATISFACTION:

It helps customers to reduce threats that happen during e-banking. Customer can enter the correct URL and all the passwords,usernames,private information, credit card details are kept safe. It will prevent from information disclosure and property damage. It will increase customer satisfaction without fearing of malicious sites.

BUSINESS MODEL (FINANCIAL BENEFIT):

Phishing detection helps in preventing from falling for malicious websites and traps. Thus ensuring the safety of one's personal data and other private informations. Doing this beforehand by detecting through ML models can save time. The proposed solution is also a low-cost model and the customers are not charged for the service they receive.

SCALABILITY OF SOLUTION:

The model’s performance is increased by building it more accurate model with the use of several classification algorithms and selecting the best accurate model among the different models run. Also, through integration of these models, an optimized hybrid model can be obtained in order to result in more scalability. Deploying the ML model into cloud also makes it easy for enterprises to experiment with the model capabilities and scale up. Placing a finished flight prediction model into a live environment can be used for its intended purpose and it is integrated with Flask, so that they can be accessed by end users.