Project Design Phase-I

Proposed Solution Template

Date	24 September 2022
Team ID	PNT2022TMID40333
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

Proposed Solution Template:

Project team shall fill the following information in proposed solution template.

S.No.	Parameter	Description
1.	Problem Statement(Problem to be solved)	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.
2.	Idea / Solution description	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.
3.	Novelty / Uniqueness	Machine learning technology consists of a many algorithms which requires past data to make a decision or prediction on future data. Using this technique, algorithm will analyze various blacklisted and legitimate URLs and their features to accurately detect the phishing websites including zero- hour phishing websites.
4.	Social Impact / Customer Satisfaction	Phishing has a list of negative effects on a business, including loss of money, loss of intellectual property, damage to reputation, and disruption of operational activities. Example: • Facebook and Google. Between 2013 and 2015, Facebook and Google were tricked out of $100 million due to an extended phishing campaign... Customer Satisfaction: • By using our web phishing detection website the user can check their websites by copy and paste the phishing URL. • After knowing the result they can be completely safe from above mentioned impacts.
5.	Business Model (Revenue Model)	As long as phishing websites continue to operate, many more people and companies will suffer privacy leaks or financial losses. Therefore, the demand for fast and accurate phishing website detection grows stronger. However, the existing phishing detection methods do not fully analyze the features of phishing, and the performance and efficiency of the models only apply to certain limited datasets and need to be improved to be applied to the real web environment.

6.	Scalability of the Solution	Features are length of an URL, URL has HTTP, URL has suspicious character, prefix/suffix, number of dots, number of slashes, URL has phishing term, length of subdomain, URL contains IP address