Project Design Phase – 1
Proposed Solution

Date	24 September 2022
Team ID	PNT2022TMID23060
Project Name	Web Phishing Detection
Maximum Marks	2 marks

Proposed Solution:

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. Common threats of web phishing: • Web phishing aims to steal private information, such as usernames, passwords, and credit card details, by way of impersonating a legitimate entity. • It will lead to information disclosure and property damage. • Large organizations may get trapped in different kinds of scams.
2.	Idea / Solution description	1. 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. 2. 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	1. Using machine learning and classification algorithms, the criteria for detecting the phishing websites are extracted. 2. The machine is trained with the extracted criteria and when the customer makes payment using e-payment website the system detects the phishing website.
4.	Social Impact / Customer Satisfaction	1. Nowadays e-payment has become most popular way of payment and many online purchases depends on e-payment. 2. The main goal is to detect the phishing e-payment website and protect user details from phishing to ensure their privacy.
5.	Business Model (Revenue Model)	1. This system generate revenue from the users and from online product selling platforms.
6.	Scalability of the Solution	1. Machine learning helps people to safely transfer their money without losing their personal details by detecting the phishing websites. 2. This makes the user to feel safe and secure to use e-payments for online purchase.