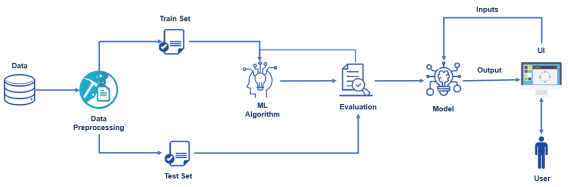
Project Design Phase-I
Proposed Solution Template

Date	19 September 2022
Team ID	PNT2022TMID45454
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

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. 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	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: 
3.	Novelty / Uniqueness	Machine Learning algorithm and Data mining algorithms used in this system provide better performance as compared to other traditional classifications algorithms.
4.	Social Impact / Customer Satisfaction	● This system can be used by many E-banking or other websites in order to have good customer relationships. ● Users can make online payments securely.
5.	Business Model (Revenue Model)	It provides cloud -based software as a service (SaaS) for organizations to detect phishing with various plans and open source for individuals.
6.	Scalability of the Solution	ML-based models are the only stream that shows the ability to detect 0-day phishing attacks while being scalable and accurate.