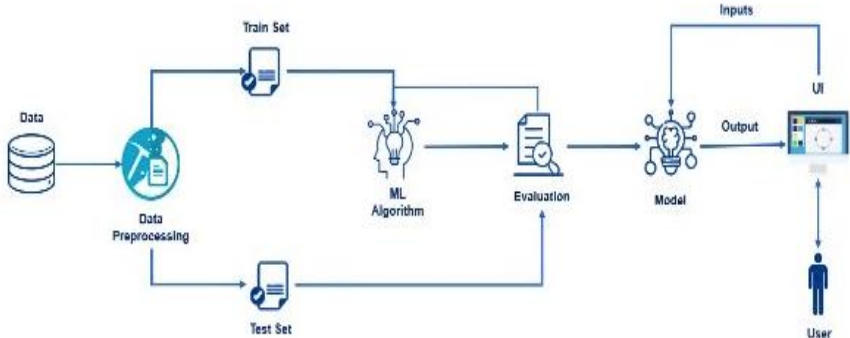


Project Design Phase - I

Date	24 September 2022
Team ID	PNT2022TMID45474
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

Proposed Solution Template :

S. No	Parameter	Description
1.	Problem Statement (Problem to be solved)	<p><u>Problem Statement :</u></p> <p>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.</p> <p>Common threats of web phishing:</p> <ul style="list-style-type: none">• 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	<p><u>Solution Description :</u></p> <p>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</p>

		<p>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.</p> <p><u>Technical Architecture :</u></p>  <pre> graph LR Data[(Data)] --> DP[Data Preprocessing] DP --> TS[Train Set] DP --> TeS[Test Set] TS --> ML[ML Algorithm] TeS --> Eval[Evaluation] ML --> Eval Eval --> Model[Model] Model --> Output[Output] Output --> UI[UI] UI --> User[User] Inputs[Inputs] --> Model </pre>
3.	Novelty / Uniqueness	Install online anti-phishing software in user's computers or like google chrome Extension.
4.	Social Impact / Customer Satisfaction	To avoiding Phishing scams & improvement in Security development. Bug free & Ads free. Continuous updates will be provide.
5.	Business Model (Revenue Model)	Single user or personal user's can use most facility of this application for free. Paid version for enterprises company's.
6.	Scalability of the Solution	It's a User friendly. Huge user's accessibility for avoidance of server traffic