Project Design Phase-I
Proposed Solution

Date	19 September 2022
Team ID	PNT2022TMID26256
Project Name	Project – Web phishing detection
Maximum Marks	2 Marks

S. No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	• It is important to be cautious while we provide sensitive data such as username, password, credit card details, personal information, etc. • As the number of users who purchase products through online and make payments through e-banking increases, the number of fraudulent e-banking websites also increases who try to get sensitive information from the users for malicious reasons. • Such a kind of an e-banking website is an example of a phishing website. • They impersonate as a legitimate entity to steal private information from us. • These activities lead to information disclosure and property damage. • Web phishing is becoming 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 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. • The real-time prediction will include whitelist filtering, blacklist interception and Machine Learning (ML) prediction.

3.	Novelty / Uniqueness	• To deal with phishing attacks and distinguishing the phishing webpages automatically, Blacklist based detection technique keeps a list of websites' URLs that are categorized as phishing sites. • If a web-page requested by a user exists in the formed list, the connection to the queried website is blocked. • Machine Learning (ML) based approaches rely on classification algorithms such as Support Vector Machines (SVM) and Decision Trees (DT) to train a model that can later automatically classify the fraudulent websites at run-time without any human intervention. • Also, in terms of UI, the website designed will be user friendly in means for any age.
4.	Social Impact / Customer Satisfaction	• The website should be designed in such a way that the user feels protected by using it as the business-related credentials will be safe by performing the detection activity. • Parents can be relaxed when kids explore educational website as the fraudulent website will be detected by our website. • Web phishing detection will help the customers to take precautionary steps to minimize the losses and consider technological solutions to improve their security measures.
5.	Business Model (Revenue Model)	• The browser plugin can be provided with a subscription plan or could be sold as a licensed software. • This can be an efficient way to help banking sector as it secures the legitimate website from other malwares that are set by hackers.
6.	Scalability of the Solution	• To create microservices with flask web framework so that the model could scaled vertically or horizontally and effective traffic management. • Preparing newsletters and CRN magazines to create an awareness about web phishing to the generations who perform online transactions.