Project Design Phase-I
Proposed Solution

Date	19 September 2022
Team ID	PNT2022TMID27147
Project Name	Project - Web Phishing Detection
Maximum Marks	2 Marks

Proposed Solution:

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	This is an interactive and responsive website that will be used to detect whether a website is legitimate or phishing. Phishing becomes a main area of concern for security researchers because it is not difficult to create the fake website which looks so close to legitimate website. Experts can identify fake websites but not all the users can identify the fake website and such users become the victim of phishing attack, as an example, passwords associate degree open-end credit unpretentious elements by presumptuous the highlights of a reliable individual or business in electronic correspondence. Phishing makes use of parody messages that square measure created to seem substantial and instructed to start out from true blue sources like money connected institutions, online business goals, etc, to draw in customers to go to phoney destinations through joins gave within the phishing websites.
2.	Idea / Solution description	Determine whether the provided URL is real or a phishing URL, and then output the answer with the proportion of risk factors.
3.	Novelty / Uniqueness	• Proposed web technology features improve phishing detection accuracy. • The usage of 10 machine learning algorithms produces the results with an accuracy of 96% approximately. • Simple, Easy-to-Understand UI. • A successful detection mechanism is developed by using an ideal dataset.

4.	Social Impact / Customer Satisfaction	• It is based on URL feature extraction that helps in detecting phishing attacks that are relatively new and which is not possible for most of the other phishing detectors. • The system involves just ten algorithms that act as filters to determine the legitimacy of the URL. • Users just need to provide the URL of the website whose legitimacy needs to be determined. Nothing else needs to be done by the user.
5.	Business Model (Revenue Model)	• B2C Model (end product sold to individuals such as children's gadgets and senior citizens at risk of assaults) and B2B Model (Machine Learning model/API can be sold to multiple enterprises for their employees) • The Application Programming Interface can be purchased in bulk by businesses at a subsidised rate (API) • Premium subscribers will get access to the URL's data and the justifications for a site's "unsafe" rating.
6.	Scalability of the Solution	• When there are more users and activity, the solution may require more hardware resources. • The API can make sure that several requests are processed in parallel at once.