Project Design Phase-I
Proposed Solution Template

Date	25 October 2022
Team ID	PNT2022TMID29369
Project Name	Project – Web phishing detection
Team Lead	Chandru S
Team Members	Ashok E Arun kumar A Purushothaman R Srihari S
Maximum Marks	2 Marks

Proposed Solution Template:

Project team shall fill the following information in proposed solution template.

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	Phishing is a major problem, which uses both social engineering and technical deception to get users' important information such as financial data, emails, and other private information. Phishing exploits human vulnerabilities; therefore, most protection protocols cannot prevent the whole phishing attacks. Many of them use the blacklist whitelist approach, however, this cannot detect zero-hour phishing attacks, and they are not able to detect new types of phishing attacks.
2.	Idea / Solution description	A common way to obtain phishing detection measurements is to perform an assessment. To continue with the phishing detection example, a measurement of how many suspicious e-mails were reported to security would be collected at the end of each phishing assessment. If you're using a commercial tool, the number of e-mails sent during each assessment is available from the reporting screen.
3.	Novelty / Uniqueness	Using the Machine learning technology to detect the phishing attacks Machine learning is one of the critical mechanisms working in tandem with Artificial Intelligence (AI). It is based on algorithms focused on understanding and recognizing patterns from enormous piles of data to create a system that can predict unusual behaviours and anomalies. It evolves with time while learning patterns of normal behaviours. These characteristics make it helpful in identifying phishing emails, spam, and malware.

4.	Social Impact / Customer Satisfaction	Millions of people are being affected and billions of dollars are getting stolen. Phishing is a technique used to extract personal

		information from victims by means of deceptive and fraudulent emails for identity theft. As a result of this, the organizations as well consumers are facing enormous social effects. Phishing is causing two-way damage.
5.	Business Model (Revenue Model)	Tool has been used to import Machine learning algorithms. Each classifier is trained using training set and testing set is used to evaluate performance of classifiers. Performance of classifiers has been evaluated by calculating classifier's accuracy score. improve the accuracy of our models with better feature extraction.
6.	Scalability of the Solution	For future enhancements, we intend to build the phishing detection system as a scalable web service which will incorporate online learning so that new phishing attack patterns can easily be learned and improve the accuracy of our models with better feature extraction.