Project Design Phase-I
Proposed Solution Template

Date	22 Septermber 2022
Team ID	PNT2022TMID42499
Project Name	Web Phishing Detection
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)	Malicious links will lead to a website that often steals login credentials or financial information like credit card numbers. Attachments from phishing emails can contain malware that once opened can leave the door open to the attacker to perform malicious behavior from the user's computer.
2.	Idea / Solution description	In order to detect and predict phishing website, we proposed an intelligent, flexible and effective system that is based on using classification Data mining algorithm. We implemented classification algorithm and techniques to extract the phishing data sets criteria to classify their legitimacy. The 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 user makes transaction through online when he makes payment through the website our system will use data mining algorithm to detect whether the website is phishing website or not. This application can be used by many E-commerce enterprises in order to make the whole transaction process secure.
3.	Novelty / Uniqueness	A novel approach that can detect phishing attack by analysing the hyperlinks found in the HTML source code of the website. The proposed approach incorporates various new outstanding hyperlink specific features to detect phishing attack. The proposed approach has divided the hyperlink specific features into 12 different categories and used these features to train the machine learning algorithms. We have evaluated the performance of our proposed phishing detection approach on various classification algorithms using the phishing and non-phishing websites dataset.
4.	Social Impact / Customer Satisfaction	With the development of the Internet, network security has aroused people’s attention. It can be said that a secure network environment is a basis for the rapid and sound development of the Internet. Phishing is an essential class of cybercriminals which is a malicious act of tricking users into clicking on phishing links, stealing user

		information, and ultimately using user data to fake logging in with related accounts to steal funds. Network security is an iterative issue of attack and defense. The methods of phishing and the technology of phishing detection are constantly being updated. Traditional methods for identifying phishing links rely on blacklists and whitelists, but this cannot identify new phishing links
5.	Business Model (Revenue Model)	A revenue model is a framework for generating financial income. It identifies which revenue source to pursue, what value to offer, how to price the value, and who pays for the value. It is a key component of a company's business model.
6.	Scalability of the Solution	Scalability is certainly a high-level problem that we will all be thrilled to have. Reaching a point where we need to incorporate more machines and resources to handle the traffic coming into our deep learning algorithm, is a dream come true for many startups. However many engineering teams don't pay the necessary attention to it. The main reason: they don't have a clear plan on how to scale things up from the beginning. And that's perfectly fine! Because we first need to focus on optimizing our application and our model, and deal with all that stuff later. But it wouldn’t hurt us to have a clear plan from the start.