Project Design Phase-I

Date	02 October 2022
Team ID	PNT2022TMID13259
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

Proposed Solution Template:

S.No.	Parameter	Description
1.	Problem Statement (Problem to besolved)	Many consumers utilize e-banking to make purchases and payments for goods they find online. There are several e-banking websites that often request sensitive information from users—such as usernames, passwords, and credit card information—for harmful purposes. Phishing websites are this kind of online banking websites. One of the most important software services for communications on the Internet is the web service. One of the many security risks to online services on the Internet is web phishing. By seeming to be a trustworthy organization, web phishing seeks to obtain sensitive information including usernames, passwords, and credit card numbers. It will result in data leakage and property damage. Large businesses may fall victim to various schemes.
2.	Idea / Solution description	A significant area for investigation is the detection and prevention of phishing websites. There are several phishing strategies that provide attackers with numerous and vital ways to access the information of individuals and companies. Locator for uniform resources URLs, which are occasionally referred to as "Web links," are crucial in phishing attacks. Uniform resource locator has the potential to reroute pages, i.e., through a hyperlink, to either a legitimate website or a phishing website. Every day, new methods for creating phishing sites appear. This in fact encouraged a number of researchers to focus their efforts on locating the phishing sites.
3.	Novelty / Uniqueness	We have thoroughly examined and determined several elements that may be utilized to recognize a phishing website. These elements can be classified as address bar-based features, domain-based features, HTML-based features, or JavaScript-based features. We can accurately detect a phishing site using these qualities.
4.	Social Impact / Customer Satisfaction	Each indexing database was subjected to a thorough, methodical search. The most recent information on web phishing detections was gathered. On the basis of the methodology, the papers were categorized. By doing a thorough scan on the top-secret documents, taxonomy was developed. The contributions described in this survey are comprehensive and include every recent advancement in this field.

5.	Business Model (Revenue Model)	Spreading fraudulent email is the first step in a phishing scan. When an online user clicks on a phishing URL or link, anti-phishing mechanisms begin to act, either by forwarding the phishing email to the spam folder or by displaying a warning. the stages of a phishing attack in this region.
6.	Scalability of the Solution	The domains of phishing sites show the characteristics that set them apart from other websites and domains. (Google, www.google.com and any other random phishing website www.google.com, are two examples.) When compared to other websites and domain names phishing Uniform Resource Locators and "domain names" frequently differ in length. This affects both the training accuracy and testing accuracy of all the models. The variance in train and test accuracy numbers demonstrates that the models are not being overfit to the extensive dataset.