Project Design Phase-I

Proposed Solution Template

Date	20 October 2022
Team ID	PNT2022TMID09754
Project Name	Project – 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)	Due to the rapid growth of the Internet, user interact with social network such as Facebook, Twitter, Linkedin and many more for communicate with each other. By using the unusual structure of the Internet, attacker set out new techniques, such as phishing, to lure the user to interact with the fake websites through social networks that appears similar to legitimate ones. The main motive behind this attack is to steal the sensitive information such as password, username, credit card details and many more details from the users. There are various platforms where phishing attack can occur like online payment sector, webmail, and financial institution, file hosting or cloud storage and many more.
2.	Idea / Solution description	This presents a methodology for phishing website detection based on machine learning classifier s with a wrapper features selection method. In this some common supervised machine learnin g d r techniques are applied with effective an significant features selected using the wrappe features selection approach to accurately detec phishing websites.

,

3.	Novelty / Uniqueness	This system is designed for resources are used as intended, prevents from valuable information from leaks out, produce better control mechanism and alerts the user to keep their private information safe.
4.	Social Impact / Customer Satisfaction	To notify the user on blacklisted website through pop-up while they are trying to access and to notify the user on blacklisted website through email while they are trying to access.

5.	Business Model (Revenue Model)	The user can be notified if blacklisted website is being accessed. The admin can capture the blacklisted URL's to alert user. The system involves features like capturing blacklisted website, viewing blacklisted website, displaying pop-up notification and also displaying email notification.
6.	Scalability of the Solution	Although the wrapper-based features selection method may consume more time and require extra computational overhead with some classifiers, the wrapper-based features selection method is usually used once in order to provide the most influential features. The machine learning classifiers should then be retrained with these selected features regularly in the update process in order to improve the efficiency and adaptability of the intelligent phishing websites detection approaches. Furthermore, the wrapperbased features selection can be used with ensemble learning to improve the performance of the intelligent phishing website detection techniques