Project Design Phase-I

Proposed Solution

Date	19 October 2022
Team ID	PNT2022TMID43237
Project Name	Web phishing Detection
Maximum Marks	2 Marks

SI.NO	PARAMETER	DESCRIPTION
1.	Problem statement (problem to be solved)	Phishing has become one of the biggest and most effective cyber threats, causing hundreds of millions of dollars in losses and millions of data breaches every year.
2.	Idea / Solution description	Phishing attacks have become a significant concern owing to an increase in their numbers. It is one of the most widely used, effective, and destructive attacks.
3.	Novelty / Uniqueness	The average person to distinguish phishing websites from normal websites because phishing websites appear similar to the websites they imitate. In many cases, users do not check the entire website URL, and, once they visit a phishing website, the attacker can access sensitive and personal information.
4.	Social impact / Customer satisfaction	The growth in the field of e-commerce, phishing attack and cybercrimes are rapidly growing. Attackers use websites, emails, and malware to conduct phishing attacks.
5.	Business model (revenue model)	Different deep learning models, such as recurrent neural network (RNN) and proposed convolutional neural network (CNN), are evaluated in this experiment on datasets D1 and D2.

6.	Scalablity of the solution	According to the results, it can be seen that the accuracy of phishing website detection by traditional machine learning-based methods on dataset D2 is significantly lower than that of the proposed method.