Project Design Phase-I

Proposed Solution

Date	19 September 2022
Team ID	PNT2022TMID10135
Project Name	Project – Web Phishing Detection
Maximum Marks	2 Marks

Proposed Solution:

S.No.	Parameter	Description
1.	Proposed Statement (Problem to be solved)	To detect the web phishing sites which steals the private information, such as usernames, passwords, and credit card details, by way of impersonating a legitimate entity using the effective machine learning algorithm.
2.	Idea / Solution Description	To detect the web phishing websites for providing secured e-banking transactions, an intelligent and effective system based on classification machine learning algorithm is proposed. Classification algorithms helps to identify the phishing datasets based on their authorised information like URL, Domain identity and encryption criteria. Once the user logs in to the e-banking websites, the proposed algorithm identifies the legitimateness of the website and blocks the phishing site.
3.	Novelty / Uniqueness	1. The proposed system is a complete AI & ML dependent system since the prevention methods used in current systems are blacklisting based method which faces the zero-hour phishing threat detection. 2. The proposed classification algorithm helps to identify the phishing site in an effective manner and blocks the site while avoiding the property damage for the users. 3. The proposed model helps users to avoid getting trapped in different

		kinds of scams. In internet e-banking and transactions set by scammers
4.	Social Impact / Customer Satisfaction	1. It will save the users from fraudulent websites and reduced global economical losses caused by web phishing every year. 2. It provides the users a highly safe and secured environment to search through internet and make payment and other activities 3. It gives a reliable way to detect web phishing and scamming sites 4. It provides a secured and Confidential environment for e-banking 5. It provides a completely Authenticated sites for users safe and protected transitions
5.	Business Model (Revenue Model)	Cyber Threat Intelligence it is a commercial web phishing protection software or web extension tool that helps and protects the user from web phishing by automatically detecting phishing sites by AI & ML based detection system Bank transactions
6.	Scalability of the solution	It will be useful for a wide range of users from individual users to corporates, banks and universities. Helps in reducing economical loss caused by these web phishing incidents and also protects from confidential and personal information losses