PROJECT DESIGN PHASE II

FUNCTIONAL REQUIREMENTS

Date	13 October 2022
Team ID	PNT2022TMID15077
Project Name	Web Phishing Detection
Maximum Marks	4 Marks

FUNCTIONAL REQUIREMENTS:

FR NO.	Functional Requirement (Epic)	Sub Requirement (Story / Sub-Task)
FR-1	User Input	User inputs an URL in required field to checkits validation.
FR-2	Website Comparison	Model compares the websites using Blacklistand Whitelist approach.
FR-3	Feature extraction	After comparing, if none found on comparison then it extracts feature using heuristic and visualsimilarity approach.
FR-4	Prediction	Model predicts the URL using MachineLearning algorithms such as Logistic Regression, KNN, SWA
FR-5	Classifier	Model sends all output to classifier and produces final result.
FR-6	Announcement	Model then displays whether website is a legalsite or a phishing site.
FR-7	Events	This model needs the capability of retrievingand displaying accurate result for a website

Non-functional Requirements:

Following are the non-functional requirements of the proposed solution

FR No.	Non-Functional Requirement	Description
NFR-1	**Usability**	Usability is commonly considered to be the enemy of security. In general, being secure means taking extra steps to avoid falling for different attacks. This is especially true of phishing where the best ways to prevent most phishing attacks are commonly known, but cybersecurity guidance is rarely followed.
NFR-2	**Security**	Implementation of updated security algorithms and techniques.
NFR-3	**Reliability**	The reliability factor evaluates if a suspected site is legitimate or not.
NFR-4	**Performance**	A phishing website has two key characteristics: it closely resembles a real website and has at least one field for users to enter their credentials. A suspicious attachment is frequently used as a phishing attempt warning sign.
NFR-5	**Availability**	A common social engineering tactic used to acquire user credentials is phishing. containing account information and payment information. It happens when an attacker deceives a victim into opening an email, instant message, or text message by disguising themselves as a reliable source.
NFR-6	**Scalability**	Scalable phishing detection and isolation, the primary ideas are to shift protection from end users to network providers and to use the innovative bad neighborhood concept to detect and isolate both phishing email and phishing web servers.