Project Design Phase-II
Solution Requirements (Functional & Non-functional)

Date	19 October 2022
Team ID	PNT2022TMID43816
Project Name	Project – WEB PHISHING DETECTION
Maximum Marks	4 Marks

Functional Requirements:

Following are the functional requirements of the proposed solution.

FR No.	Functional Requirement (Epic)	Sub Requirement (Story / Sub-Task)
FR-1	User Registration	Registration through Form Registration through Gmail Registration through Linkedin
FR-2	User Confirmation	Confirmation via Email Confirmation via OTP
FR-3	User Authentication	Confirmation for Email Confirmation for Password
FR-4	User Security	Strong password Two step verifications Updating device management
FR-5	User Performance	Official websites use Internet usage limitation Sharing information
FR-6	Extraction and Prediction	It retrieves features based on heuristics and visual similarities. The URL is predicted by the model using Machine Learning methods such as Logistic Regression and KNN.
FR-7	Real Time monitoring	The use of Extension plugin should provide a warning pop-up when they visit a website that is phished. Extension plugin will have the capability to also detect latest and new phishing websites.

Non-functional Requirements:

Following are the non-functional requirements of the proposed solution.

FR No.	Non-Functional Requirement	Description
NFR-1	**Usability**	User can have full access to the particular websites they using must proceed some certain user-friendly websites so that it does not affect the data.
NFR-2	**Security**	To check whether the particular website is secure or not we can notify it by displaying an alert box while using the websites.
NFR-3	**Reliability**	It must be a reliable source to the users while they using the websites.
NFR-4	**Performance**	The performance of web phishing detection is high and it is very efficient as it is too easy to understand and has a high security and scalability.
NFR-5	**Availability**	Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, impersonate as a trusted entity, dupes a victim into opening an email, instant message, or text message.
NFR-6	**Scalability**	The main ideas are to move the protection from end users towards the network provider and to employ the novel bad neighbourhood concept, in order to detect and isolate both phishing e-mail senders and phishing web servers.