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

Team ID	PNT2022TMID49306
Project Name	Web phishing detection

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 Execution	Verify via Email
FR-4	Completion process	Successfully completed

Non-functional Requirements:

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

FR No.	Non-Functional Requirement	Description
NFR-1	**Usability**	An internet user can be access in the information process with an environment
NFR-2	**Security**	The real measure of training effectiveness comes when we evaluate explicit measures of our success. In many cases, this will mean developing metrics that we can use for such evaluation
NFR-3	**Reliability**	Data wiping or destruction Number of users properly following data destruction policies/processes.
NFR-4	**Performance**	A novel technique called Syntactical Fingerprinting is used to compare structural components, or constructs, within files to determine whether the files are similar enough to be of the same provenance and thus belong to the same file family.
NFR-5	**Availability**	thus, software-based phishing detection techniques are preferred for fighting against the phishing attack. Mostly available methods for detecting phishing attacks are blacklists/whitelists5, natural

		language processing6, visual similarity7, rules8, machine learning techniques 9,10,
NFR-6	**Scalability**	Feature engineering, feature taxonomy, framework, phishing email, phishing URL, phishing website.