Project Design Phase-II
Functional Requirements

Date	30 Oct 2022
Team ID	PNT2022TMID10245
Project Name	Project - 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 Registrationthrough LinkedIN Registration through websites.
FR-2	User Confirmation	Confirmation via Email Confirmation via OTP
FR-3	User Authentication	Confirmation for email. Confirmation for passwords
FR-4	User Security	Strong Passwords, Two factor authentication, updating device management
FR-5	User Performance	Usage of legitimate websites, optimize network traffic.

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 bestways to prevent most phishing attacks are commonly known, but cybersecurity guidance is rarely followed.
NFR-2	**Security**	Implementation of updated security algorithmsand techniques.
NFR-3	**Reliability**	The reliability factor evaluates if a suspected siteis legitimate or not.
NFR-4	**Performance**	A phishing website has two key characteristics: it closely resembles a real website and has at leastone 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 intoopening 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 endusers to network providers and to use the innovative bad neighbourhood concept to detect and isolate both phishing email and phishing web servers.