Project Design Phase-II

Solution Requirements (Functional & Non-functional)

Date	25 October 2022
Team ID	PNT2022TMID37408
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 OT
FR-3	User Authentication	Confirmation of Google Firebase
FR-4	User Security	Strong Passwords , 2FA and FIDO2.0 Webaucn
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**	Responsive UI / UX Design and users can easily configure the settings based on their preference.
NFR-2	**Security**	Implementation of Updated security algorithms and techniques.
NFR-3	**Reliability**	Reliability Factor determines the possibility of a suspected site to be Valid or Fake.
NFR-4	**Performance**	The two main characteristics of a phishing site are that it looks extremely similar to a legitimate site and that it has at least one field to enable users to input their credentials.
NFR-5	**Availability**	It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.
NFR-6	**Scalability**	Scalable detection and isolation of phishing, 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