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

Date	23 October 2022
Project Name	Web Phishing Detection
Team ID	PNT2022TMID37334
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 Gmail Registration by creating a new user name and password
FR-2	User Confirmation	Confirmation via Email Confirmation via OTP
FR-3	User login	Login creates a user account. Should have two text field(LOGIN NAME,PASSWORD)
FR-4	User permission	Permissions allow a user to view information related to a function, or view and change information related to a function. Roles are named groups of permissions that can be assigned to users.
FR-5	Using the intelligent system	User will use the intelligent system to detect phishing websites and save himself from his money being looted

Non-functional Requirements:

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

FR No.	Non-Functional Requirement	Description
NFR-1	**Usability**	It is very user friendly, any people with less knowledge also can easily understand that they are using the fake website through our alert message.
NFR-2	**Security**	It is very secured as one cannot hack our detection website so one can easily trust our detection website and they will be saved from financial and information loss.
NFR-3	**Reliability**	a phishing detection system, which provided recommendations to users as to whether an email was legitimate or phishing, was used as the automation system. The reliability of this system was defined as **the percentage of times when the system was correct identifying the emails** (60%, 70%, 80%, 90%).
NFR-4	**Performance**	The performance of web phishing detection is high and it is very efficient and scalable

| NFR-5 | Availability | This detection website is available at any system like laptop , mobile phone , desktop and user friendly |

NFR-6	**Scalability**	The total execution time of our approach in phishing webpage detection is around 2-3 sec, which is quite less and acceptable environment. As input size increases the execution time increases and this makes the system difficult to handle increases the stress.