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

Date	03 October 2022
Team ID	PNT2022TMID26146
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
FR-2	User Confirmation	Confirmation via Email Confirmation via OTP
FR-3	Website Evaluation	The model evaluates the website that has been entered by the user to check whether it is malicious or not.
FR-4	Prediction	The model predicts the malicious website using machine learning algorithms.
FR-5	Authentication-Results	The model predicts the website based on the evaluation results and alerts the user before providing any confidential information

Non-functional Requirements:

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

FR No.	Non-Functional Requirement	Description
NFR-1	**Usability**	Usability is a quality attribute that assesses how easy user interfaces are to use. In web phishing, users can use the website without any fear of losing their own credentials
NFR-2	**Security**	Security refers to protecting and securing users'a, networks, and software, from unauthorized access, misuse, theft, information loss, and other security issues. Here, users will be able to access the website without losing confidential data to an unauthorized person.
NFR-3	**Reliability**	Reliability is the probability that a product, system, or service will perform its intended function adequately for a specified period or will operate in a defined environment without failure. The website should detect phishing websites accurately without confusion.

NFR-4	**Performance**	Performance defines how fast a software system or a particular piece of it responds to certain users' actions under a certain workload. In most cases, this metric explains how long a user must wait before the target operation happens given the overall number of users now.
NFR-5	**Availability**	Availability describes how likely the system is accessible to a user at a given point in time. The phishing detection application must be readily available to detect the websites and intimate the user any time. There shouldn't be any delay in terms of responsiveness of web application.
NFR-6	**Scalability**	Scalability is the ability of the application to handle an increase in workload without performance degradation, or its ability to quickly enlarge. It is the ability to enlarge the architecture to accommodate more users, more processes, more transactions, and additional nodes and services as the business requirements change and as the system evolves to meet the future needs of the business. In web phishing detection, the increase in end users should not lead to decrease in performance. It must also diversify different sources of phishing (emails, websites) from vast number of users.