**Project Design Phase-II**

**Solution Requirements (Functional & Non-functional)**

|  |  |
| --- | --- |
| Date | 03 October 2022 |
| Team ID | PNT2022TMID11612 |
| Project Name | 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 OTP |
| FR-3 | User Security | Strong password  Two factor authentication  Updating Device on time |
| FR-4 | User Authentication | Confirmation for email.  Confirmation for password |
| FR-5 | User Performance | Optimize network traffic, Usage of genuine websites. |

**Non-functional Requirements:**

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

|  |  |  |
| --- | --- | --- |
| **FR No.** | **Non-Functional Requirement** | **Description** |
| NFR-1 | **Usability** | Any website must accepted for detection |
| NFR-2 | **Security** | Implementation of the update security algorithms and techniques. |
| NFR-3 | **Reliability** | The web phishing websites must detected accurately and the result must be reliable. |
| NFR-4 | **Performance** | The performance must be in user friendly |
| NFR-5 | **Availability** | A common social engineering tactic is used to acquire user credentials is phishing. Containing account information and payment information. It happens when an attacker deceives a victim into opening an email, instant message, or text message by disguising themselves as a reliable source. |
| NFR-6 | **Scalability** | It must be able to handle increase in the number of users. |