**Project Design Phase-II**

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

|  |  |
| --- | --- |
| Date | 03 October 2022 |
| Team ID | PNT2022TMID37389 |
| 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 OTP |
| FR-3 | Feature extraction | After comparing, if none found on comparison then it extracts feature using heuristic and visual similarity approach. |
| FR-4 | Prediction | Model predicts the URL using Machine Learning algorithms such as Logistic Regression, KNN |
| FR-5 | Classifier | Model sends all output to classifier and produces final result. |
| FR-6 | Announcement | Model then displays whether website is a legal site or a phishing site. |

**Non-functional Requirements:**

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

|  |  |  |
| --- | --- | --- |
| **FR No.** | **Non-Functional Requirement** | **Description** |
| NFR-1 | **Usability** | Phishing is considered as one of the most serious threats for the Internet and e-commerce. Phishing attacks abuse trust with the help of deceptive e-mails, fraudulent web sites and malware. In order to prevent phishing attacks some organizations have implemented Internet browser toolbars for identifying deceptive activities. |
| NFR-2 | **Security** | A measurement for phishing detection is the number of suspicious e-mails reported to the security team. This measurement is designed to evaluate the number of employees who followed the proper procedure for reporting suspicious messages. |
| NFR-3 | **Reliability** | Web phishing aims to steal private information, such as usernames, passwords, and credit card details, by way of impersonating a legitimate entity. It will lead to information disclosure and property damage. This paper mainly focuses on applying a deep learning framework to detect phishing websites. |
| NFR-4 | **Performance** | Software-based phishing detection techniques are preferred for fighting against the phishing attack. Mostly available methods for detecting phishing attacks are blacklists/whitelists5, natural language processing6, visual similarity7, rules8, machine learning techniques |
| NFR-5 | **Availability** | Phishing is one of the biggest threats in this era of the internet. Phishing is a smart mechanism where a legitimate website is cloned and victims are lured to a fake website to provide their personal as well as confidential information, sometimes it is expensive. |
| NFR-6 | **Scalability** | This project’s performance rate will be high and it also provide many capabilities to the user without reducing its efficiency to detect the malicious websites. thus scalability of this project will be high. |