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

| | |
|---|---|
| Date | 14 October 2022 |
| Team ID | PNT2022MID12640 |
| Project Name | Project - Web Phishing Detection |
| Maximum Marks | 2 Marks |

**Functional Requirements:**

Following are the functional requirements of the proposed solution.

| FR No: | Functional Requirements and description |
|---|---|
| **FR-1** | **Feature extraction:**<br>Website URLs are present in different forms containing a variety of individual characteristics that make them unique. **The ability to extract these characteristics as features that an ML model can learn** is a topic of boundless research in the field of deep learning. |
| **FR-2** | **Website:**<br>Web hosting **makes the files that compromise a website available for viewing online**. Every website ever hosted on the internet runs on a server. The main types of hosting are shared, dedicated, VPS and reseller. |
| **FR-3** | **Web Phishing Dataset**:<br>This is a dataset that has been **used as a standard benchmark to train and test phishing detection solutions**. It contains various features that an URL would possess. |
| **FR-4** | **Cloud:**<br>The cloud provides a number of IT services such as servers, databases, software, virtual storage, and networking, among others. **It allows you to store and access your data over the internet without any limitations.** |

**Non-Functional Requirements:**

Following are the functional requirements of the proposed solution.

| NFR No: | Non-Functional Requirements and description |
|---|---|
| NFR-1 | **Usability:**<br>URL feature extraction is one of the practically important issues in phishing website detection applications. The applications of web phishing detection include **email, online payment portals, banking websites, etc** |
| NFR-2 | **Reliability:**<br>The system not only produces a classification of the phishing URLs but also a rich description of the features contributing to the co-relation mapping |
| NFR-3 | **Web Phishing Dataset**:<br>This is a dataset that has been used as a standard benchmark to train and test phishing detection solutions. It contains various features that an URL would possess. |
| NFR-4 | **Accuracy:**<br>The proposed solution is able to classify websites to be phishing or not with an accuracy of 97%. |