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

Date	28 October 2022
Team ID	PNT2022TMID34830
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	Learning & Detection	The samples and the topological structure of the machine learning TensorFlow is built. The submitted URLs are tested against the samples in the database to perform classification.
FR-2	Testing & Alert	URLs passed through the system are recorded in a database, thus each URL submitted by the user is tested to check or duplicate. If a phishing website is detected the popup message will alert the user. Give information about the malicious website with accurate result.
FR-3	Deep Learning	The phishing detection process could be done using the Recurrent Neural Network. The website could be detected.
FR-4	Hardware Requirements	2GB RAM(minimum) 100GB HDD(minimum) Intel i3 quad core 1.66GHz processor(minimum) Internet Connectivity
FR-5	Software Requirements	Windows 7 or higher Python 3.6.0 or higher Visual Studio Code Flask (python platform) HTML Dataset consisting of Phishing websites and their features Required plugins and libraries Jupiter notebook
FR-6	Other requirements	IBM cloud login Chrome extension features

Non-functional Requirements:

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

FR No.	Non-Functional Requirement	Description
NFR-1	**Usability**	This system is really used as it can able to detect phishing websites. By detecting malicious websites, our personal and professional data are confidential, secure, and accessible.
NFR-2	**Security**	Phishers spoof legitimate emails so that the victim trusts them. They send out massive numbers of fraudulent emails in order to catch a small percentage of recipients off guard. They create a sense of urgency so that the victim does not think twice before clicking the link or downloading the attachment. Lack of security awareness among employees is also one of the major reasons for the success of phishing. Organizations should be aware of how the benefits and purpose of security awareness training can secure their employees from falling victim to phishing attacks.
NFR-3	**Reliability**	The performance of the system would be accurate. Probability of giving false information is very low. As the system is working based on the deep learning algorithm, it would easily predict and give the perfect information.
NFR-4	**Performance**	The effectiveness of these methods relies on feature collection, training data, and classification algorithms and giving alerts when phished websites are detected. It must be processed and executed within a fraction of a second using the deep learning algorithm
NFR-5	**Availability**	The availability of the solution is effective and it should be helpful in a great way to prevent our personal data to be exposed.
NFR-6	**Scalability**	This solution is scalable enough to fit the Security issues by constructing the best website. The cost of establishing the website and maintaining all the programs may be high. It is acceptable to fit them over any place and any resources.