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

Date	03 October 2022
Team ID	PNT2022TMID47961
Project Name	Project – Web phishing detection
Maximum Marks	4 Marks

Functional Requirements:

FR No.	Non-Functional Requirement	Description
NFR-1	**Usability**	Share threat intelligence Remain alert about the latest threats and phishing attack tactics in your industry by sharing threat intelligence with partners and networks.
NFR-2	**Security**	Obtained centralized visibility to detect, investigate and respond to your most critical organization-wide cyber security threads with SIEM

NFR-3	**Reliability**	Our research demonstrates that current phishing detection technologies have an accuracy rate between 70% and 92.52%. The experimental results prove that the accuracy rate of our proposed model can yield up to 95%, which is higher than the current technologies for phishing website detection

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		
FR-4		

Non-functional Requirements:

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

NFR-4	**Performance**	Rules were extracted from the Random Forest Model and embedded into a Google chrome browser extension called PhishNet. PhishNet is built during the course of this research using web technologies such as HTML, CSS, and Javascript. As a result, PhishNet facilitates highly efficient phishing detection for the web.

NFR-5	**Availability**	In some cases, it may not be useful to use some of these, so there are some limitations for using these features. For example, it may not be logical to use some of the features such as Content-Based Features for the developing fast detection mechanism which is able to analyze the number of domains between 100.000 and 200.000. Another example would be, if we want to analyze new registered domains Page-Based Features is not very useful. Therefore, the features that will be used by the detection mechanism depends on the purpose of the detection mechanism. Which features to use in the detection mechanism should be selected carefully.
NFR-6	**Scalability**	This paper presents a proposal for scalable detection and isolation of phishing. The main ideas are to move the protection from end users towards the network provider and to employ the novel bad neighbourhood concept, in order to detect and isolate both phishing email senders and phishing web servers.