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

Date	22 October 2022
Team ID	PNT2022TMID27211
Project Name	WEB PHISING 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 via form Registration via Gmail Registration via LinkedIN
FR-2	User Confirmation	Confirmation via Email Confirmation via OTP
FR-3	User login	Extension plugin ability to present the pop-up to the users screen should be quick enough to the point, users will be aware before entering any confidential or sensitive details into a phishing website.
FR-4	User interaction	Extension plugin should not need the facilities and services from an 3rd party service or APIs, due the reason that those services will always the potential to leak users browsing data and pattern when it gets compromised by hackers
		Extension plugin will have the capability to also detect latest and new phishing websites

Non-functional Requirements:

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

FR No.	Non-Functional Requirement	Description
NFR-1	**Usability**	Graphical User Interface design Interface developed should be done with the understanding that it must meet the simplicity of what users would like to see when they need an extension for detecting things, and also it needs to adhere to non IT literate users as well.
NFR-2	**Security**	It must also provide the exact information on what the user wants like identifying a phishing website quickly without needing to click on many options. The process of identifying phishing website should be taken directly from the web-page user wants to view through their URL and the result from it should be easily understood by the users
NFR-3	**Reliability**	Most importantly, the extension plugin should have a popup that will notify the user regarding the website status of being phished. Software requirements: Once this is successfully achieved, a warning notification through a pop-up can be displayed towards the user, if the web-page the user is visiting is considered phishing. The process implementation of this extension plugin is very lite towards users computers and as well it gives the capability to detect phishing website in a quick effective manner.
NFR-4	**Performance**	Decision tree begins its work by choosing best splitter from the available attributes for classification which is considered as a root of the tree. Algorithm continues to build tree until it finds the leaf node. Decision tree creates training model which is used to predict target value or

		class in tree representation each internal node of the tree belongs to attribute and each leaf node of the tree belongs to class label.
NFR-5	**Availability**	The website shows information regarding the services provided by us. It also contains information regarding ill- practices occurring in todays technological world. The website is created with an opinion such that people are not only able to distinguish between legitimate and fraudulent website, but also become aware of the mal-practices occrring in current world. They can stay away from the people trying to exploit ones personal information, like email address, password, debit card numbers, credit card details, CVV, bank account numbers, and the list goes on
NFR-6	**Scalability**	Phishing detection schemes which detect phishing on the server side are better than phishing prevention strategies and user training systems. These systems can be used either via a web browser on the client or through specific host-site software presents the classification of Phishing detection approaches. Heuristic and ML based approach is based on supervised and unsupervised learning techniques. It requires features or labels for learning an environment to make a prediction. Proactive phishing URL detection is similar to ML approach. However, URLs are processed and support a system to predict a URL as a legitimate or malicious Blacklist and Whitelist approaches are the traditional methods to identify the phishing sites The exponential growth of web domains reduces the performance of the traditional method