

Team ID:PNT2022TMID29369
Project Name:Web Phishing Detection
Team Lead:Chandru S
Team Members:Srihari,Ashok,Arun Kumar,purushothaman

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

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 Websites.
FR-2	User Confirmation	Confirmation via Email. Confirmation via OTP.
FR-3	User Authentication	Confirmation for Email. Confirmation for Passwords.
FR-4	User Security	Strong passwords. Two step verifications. Updating device management.
FR-5	User Performance	Official websites use. Internet usage limitation. Sharing informations.

Non-functional Requirements:

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

FR No.	Non-Functional Requirement	Description
NFR-1	Usability	Usability is commonly considered to be the enemy of security. In general, being secure means taking extra steps to avoid falling for different attacks. This is especially true of phishing where the best ways to prevent against most phishing attacks are commonly known, but cybersecurity guidance is rarely followed.

NFR-2	Security	Phishing is a type of cybersecurity attack during which malicious actors send messages pretending to be a trusted person or entity. Lack of security awareness among employees is also one of the major reasons for the success of phishing.
-------	-----------------	--

NFR-3	Reliability	Reliability Factor is determined on the basis of the outcome of these strata, using Rough Set Theory . Reliability Factor determines the possibility of a suspected site to be Valid or Fake. Using Rough set Theory most and the least influential factors towards Phishing are also determined.
NFR-4	Performance	The two main characteristics of a phishing site are that it looks extremely similar to a legitimate site and that it has at least one field to enable users to input their credentials. A common indicator of a phishing attempt is a suspicious attachment.
NFR-5	Availability	Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.
NFR-6	Scalability	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 e-mail senders and phishing web servers.

