PROJECT DESIGN PHASE 2

FUNCTIONAL REQUIREMENTS

DATE:	05/10/2022
TEAM ID:	PNT2022TMID36177
TEAM MEMBERS:	04
PROJECT NAME:	WEB PHISHING DETECTION

FUNCTIONAL REQUIREMENTS:

FR No.	Functional Requirement (Epic)	Sub Requirement (Story / Sub-Task)
FR-1	User Input	User inputs an URL in required field to check its validation. Phisers also imitate the URLs of legitimate websites by changing many unnoticeable characters , e.g., “www.icbc.com” .
FR-2	Website Comparison	Model compares the websites using Blacklist /Whitelist approach ,natural processing, visual similarity, rules, machine learning techniques.
FR-3	Feature extraction	After comparing, if none found on comparison then it extracts feature using heuristic and visual similarity approach We have introduced eleven hyperlink features (F3–F13), two login form features (F14 and F15), character level TF-IDF features (F2), and URL character sequence features (F1).
FR-4	Prediction	Model predicts the URL using Machine Learning algorithms such as Logistic Regression, KNN . Convenient for our proposed feature set for the prediction of phishing websites, thus it has high performance.

FR-5	Classifier	Model sends all output to classifier and produces final result. XGBoost classifier is a type of ensemble classifiers , that transform weak learners to robust ones.
FR-6	Announcement	Model then displays whether website is a legal site or a phishing site.
FR-7	Events	This model needs the capability of retrieving and displaying accurate result for a website. Extract features from third-party services, search engines, website traffic, etc.