Project Design Phase-II

Technology Stack (Architecture & Stack)

Date	17 October 2022
Team ID	PNT2022TMID01009
Project Name	Web Phishing Detection
Maximum Marks	4 Marks

Technical Architecture:

The Deliverable shall include the architectural diagram as below and the information as per the table1 & table 2.

Model For Web Phishing Detection:

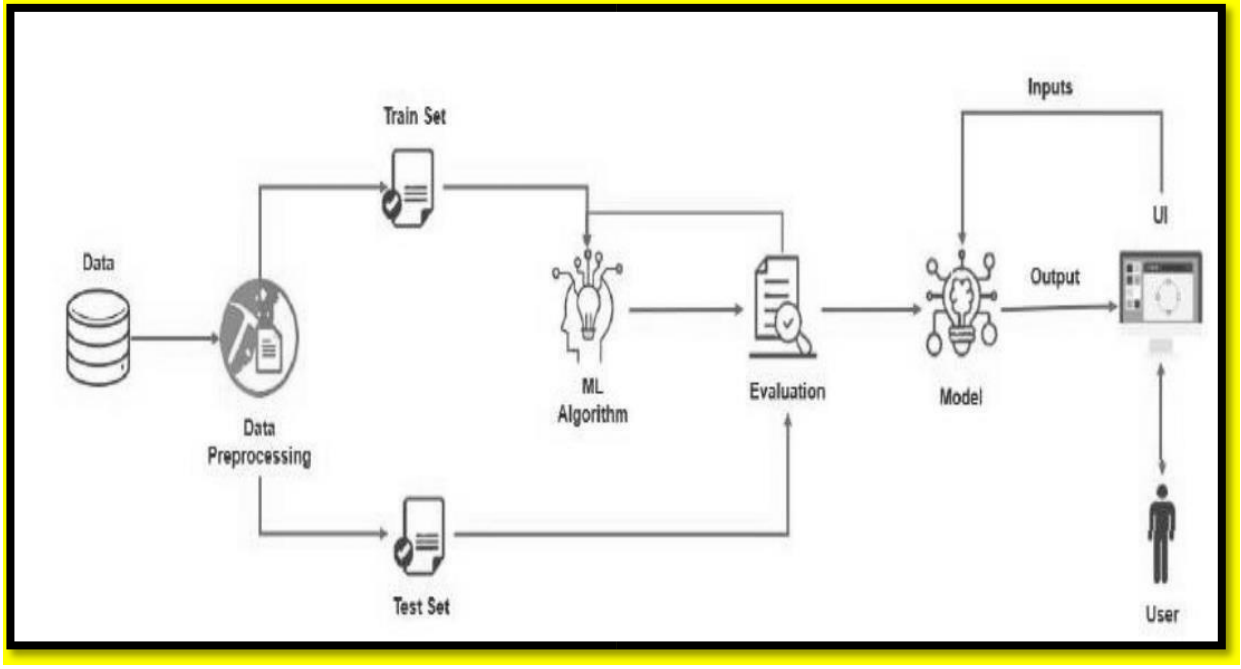

Table-1: Components & Technologies:

S.No	Component	Description	Technology
1.	User Interface	How user interacts with application e.g. Web UI, Mobile App, Chatbot etc.	HTML, CSS, JavaScript / Angular Js / React Js etc.
2.	Application Logic-1	Logic for a process in the application	Java / Python

3.	Application Logic-2	Logic for a process in the application	IBM Watson STT service
4.	Application Logic-3	Logic for a process in the application	IBM Watson Assistant
5.	Database	Data Type, Configurations etc.	MySQL, NoSQL, etc.
6.	Cloud Database	Database Service on Cloud	IBM DB2, IBM Cloudant etc.
7.	File Storage	File storage requirements	IBM Block Storage or Other Storage Service or Local File system

Table-2: Application Characteristics:

S.No	Characteristics	Description	Technology
1.	Open-Source Frameworks	Go phish is a powerful, open-source phishing framework that makes it easy to test your organization's exposure to phishing.	Machine Learning.
2.	Security Implementations	Our prototype currently includes a C#.Net implementation of a web browser.	Cofense PDR (Phishing Detection and Response)
3.	Scalable Architecture	Scalability is maximum due to accurate estimation.	jQuery, cloud flare, Bootstrap.

4.	Availability	Mostly available methods for detecting phishing attacks are blacklists/whitelists, natural language processing, visual similarity, rules, machine learning techniques	Ghost Phisher, King Phisher.
5.	Performance	We assessed the performance of the phishing classification models employing accuracy, precision, recall and F-score.	Hardware and support systems, software applications.