Project Design Phase-II

Technology Stack (Architecture & Stack)

Date	3 October 2022
Team ID	PNT2022TMID00733
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.

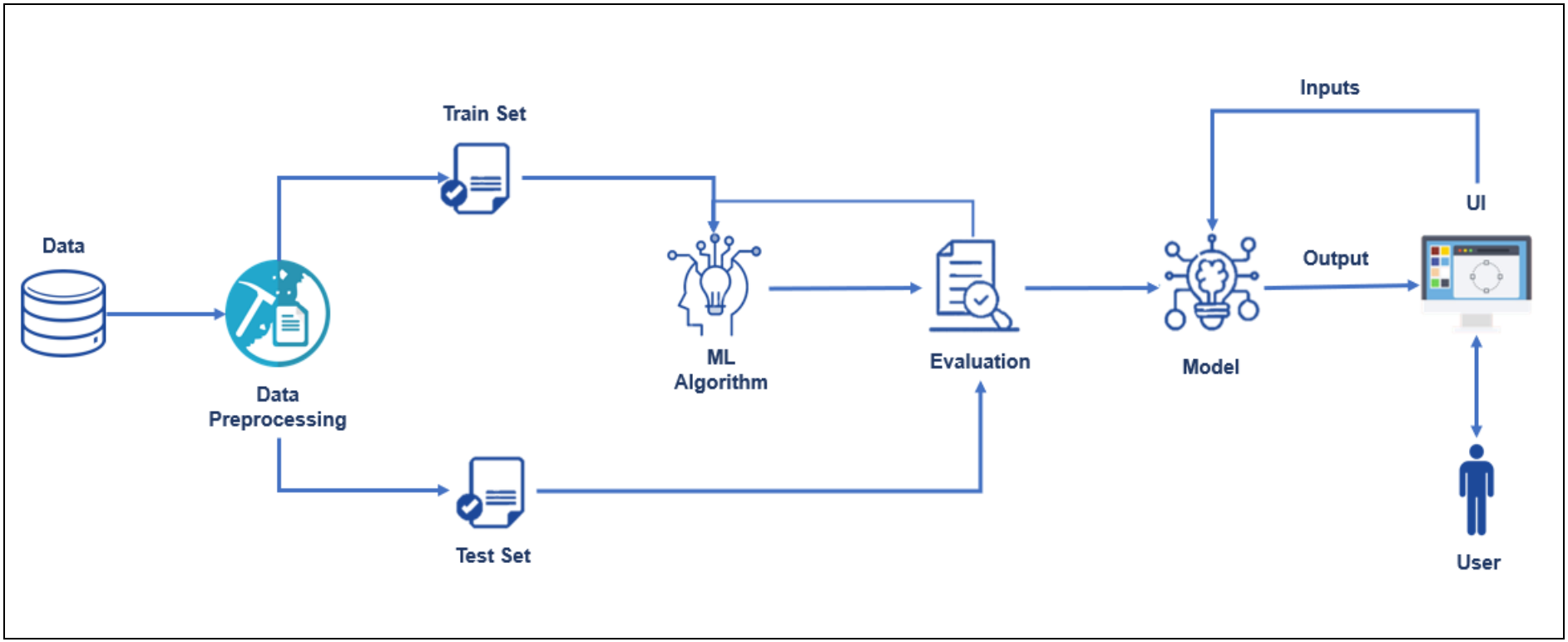

Table-1: Components & Technologies:

S.No	Component	Description	Technology
1.	User Interface	The user interacts with the application through the Web UI.	HTML, CSS, JavaScript, Flask
2.	Application Logic-1	The logic for the application is written using the Python language.	Python
3.	Application Logic-2	Machine learning models are used in order to predict the phishing and legitimate url.	Machine Learning
4.	Application Logic-3	To Deploy the model on the IBM cloud.	IBM Watson Studiio
5.	Database	The data's are collected and stored in the csv file.	SQL
6.	Cloud Database	The IBM cloud object storage service is used to store the dataset on the cloud.	IBM Cloud Object Storage Service
7.	File Storage	The codings are written on the jupyter notebook and stored as the ipynb file.	Local File System

S.No	Component	Description	Technology
8.	External API-1	IBM Watson Studio is used to run the jupyter notebook.	IBM Watson Studio
9.	External API-2	In order to train the model, we make use of Machine Learning Service.	Machine Learning Service
10.	Machine Learning Model	A machine learning model is a file that has been trained to recognize certain types of patterns.	Machine Learning Classification models
11.	Infrastructure (Server / Cloud)	Application Deployment on Local System / Cloud Local Server Configuration: Cloud Server Configuration: IBM Cloud Service.	Local, Cloud Foundry, Kubernetes, etc.

Table-2: Application Characteristics:

S.No	Characteristics	Description	Technology
1.	Open-Source Frameworks	Jupyter Notebook is a web-based open-source software for creating & sharing the documents and Flask is a web development framework.	Jupyter Notebook, Flask
2.	Security Implementations	Security / access controls implemented, use of firewalls etc.	Anti-phishing protection and anti-spam software, Firewalls, etc.
3.	Scalable Architecture	Scalability Detection and Isolation of Phishing.	Response Time, Throughput, CPU and network usages, etc
4.	Availability	The Web Application should be accessible whenever users request accessing either it by browsers or Mobile Application.	IBM Cloud
5.	Performance	Design consideration for the performance of the application and methods for detecting phishing attacks.	Blacklists/whitelists, Natural language Processing, Visual similarity, rules, machine learning techniques, etc**.**