PROJECT DESIGN PHASE - 2

TECHNOLOGY STACK

DATE	**14 October 2022**
TEAM ID	**PNT2022TMID03756**
PROJECT NAME	**WEB PHISHING DETECTION**

TECHNICAL ARCHITECTURE :

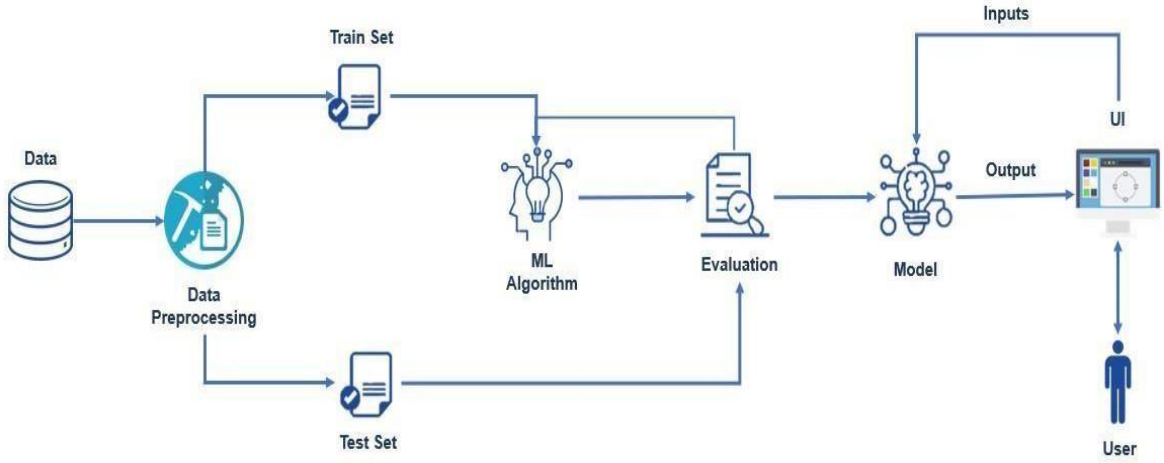

Table-1: Components & Technologies:

S.No	Component	Description	Technology
1.	Application Logic-1	Logic for a process in the application	Python
2.	Application Logic-2	Logic for a process in the application	IBM Watson STT service
3.	Application Logic-3	Logic for a process in the application	IBM Watson Assistant
4.	Database	Data Type, Configurations etc.	MySQL, NoSQL, etc.
5.	Cloud Database	Database Service on Cloud	IBM DB2, IBM Cloud ant etc.
6.	File Storage	File storage requirements	IBM Block Storage or Other Storage Service or Local Filesystem
7.	Machine Learning Model	Purpose of Machine Learning Model	Object Recognition Model, etc.
8.	Infrastructure (Server / Cloud)	Application Deployment on Local System / Cloud Local Server Configuration: Cloud Server Configuration :	Local, Cloud Foundry, Kubernetes, etc.

Table-2: Application Characteristics:

S.No	*Characteristics*	*Description*	*Technology*
1.	Open-Source Frameworks	Open-source phishing framework thatmakes it easy to test your organization's exposure to phishing.	Go phish, Speed Phish Framework(SPF), King Phisher, etc.
2.	Security Implementations	Security / access controls implemented,use of firewalls etc.	e.g. anti-phishing protection and anti-spam software etc.
3.	Scalable Architecture	Scalability detection and Isolation of phishing.	Response time, Throughput, CPU and network usages, etc.
4.	Performance	Design consideration for the performance of the application and methods for detecting phishing attacks.	Blacklists/whitelists, Natural language Processing