Project Design Phase-II
Technology Stack (Architecture & Stack)

Date	03 October 2022
Team ID	PNT2022TMID26156
Project Name	Web Phishing Detection
Maximum Marks	4 Marks

Technical Architecture:

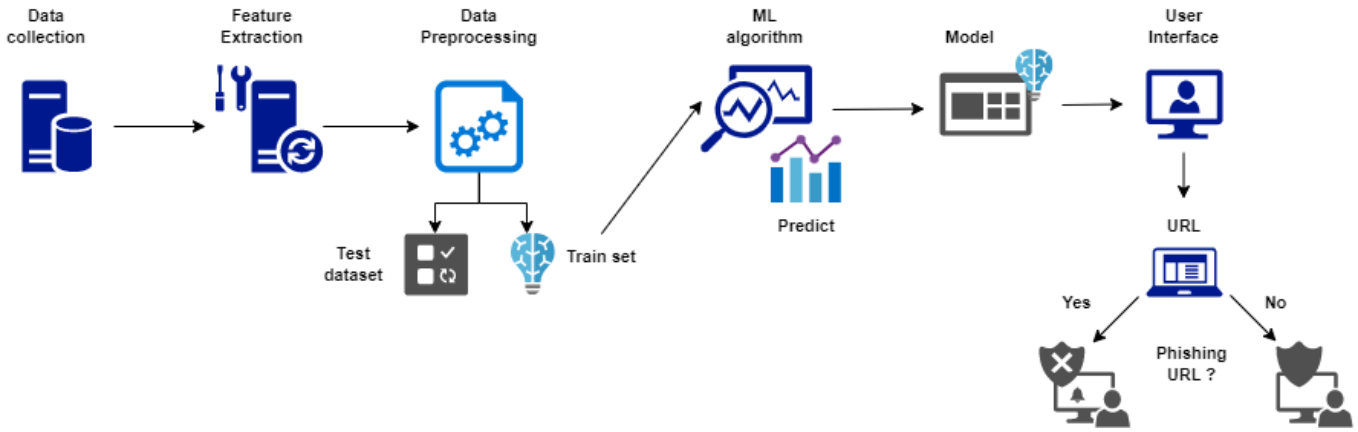

Table-1: Components & Technologies

S.No	Component	Description	Technology
1.	User Interface	The user interacts with application For example: Web UI	HTML, CSS, JavaScript
2.	Application Logic	Predict if the given URL is genuine or not.	Python, Flask API
3.	Database	Stores user input in a storage device called database.	MySQL
4.	Cloud Database	Database Service on Cloud	IBM DB2 or IBM Cloudant
5.	File Storage	Store training and testing datasets.	Local Filesystem
6.	Machine Learning Model	Classify genuine and phishing URLs.	Classification model
7.	Infrastructure (Server or Cloud)	Application Deployment on Local System or Cloud	Local, Cloud

Table-2: Application Characteristics

S.No	Characteristics	Description	Technology
1.	Open-Source Frameworks	Open-source frameworks used is deep learning.	PYTORCH
2.	Security Implementations	User launches a web browser and opens email. The backend phishing detection engine will check the email before it is opened.	Spoofing detection, fraud detection, filtering/blocking technology.
3.	Scalable Architecture	We consider creating a self-management architecture that will allow ISPs to safeguard their customers from phishing scams.	Machine learning algorithm
4.	Availability	Laptops, tablets, and mobile devices will all be compatible with this service.	Evaluation training dataset, Data pre-processing.
5.	Performance	The system needs to be quick and precise to handle all potential mistakes in a way that prevents data loss and extended periods of outage. Without any errors, the system should be able to handle many photographs, a lot of data, and many users.	Deep learning and cloud storage