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

Date	03 October 2022
Team ID	PNT2022TMID33764
Project Name	Project - Web Phishing Detection
Maximum Marks	4 Marks

Technical Architecture:

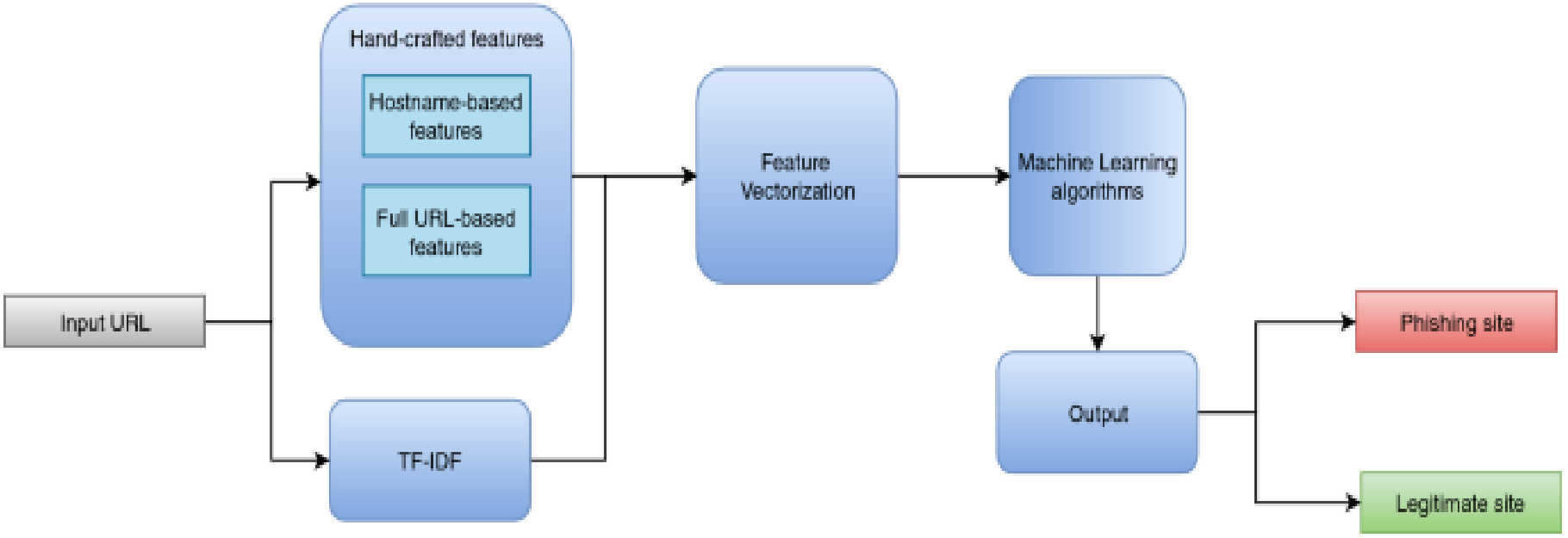

Table-1 : Components & Technologies:

S.No	Component	Description	Technology
1.	User Interface	How user interacts with application e.g. Web UI, Mobile App, Chatbot etc.	HTML, CSS, JavaScript
2.	Application Logic-1	Logic for a process in the application	Python
3.	Application Logic-2	Logic for a process in the application	Flask Server on IBM Cloud
4.	Application Logic-3	Logic for a process in the application	IBM Watson Assistant
5.	Database	Data Type, Configurations etc.	MongoDB
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 Filesystem
8.	Machine Learning Model	Purpose of Machine Learning Model	Logical Regression Model, etc.
9.	Infrastructure (Server / Cloud)	Application Deployment on Local System / Cloud Local Server Configuration: Cloud Server Configuration :	Local, Render, IBM Cloud , etc.

Table-2: Application Characteristics:

S.No	Characteristics	Description	Technology
1.	Open-Source Frameworks	Gopish 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 includes a c#.Net framework implementation of a web browser.	Cofense PDR (Phishing Detection and Response)
3.	Scalable Architecture	Scalability is maximum due to accurate estimation	jQuery,cloud flare, Bootstarp
4.	Availability	Mostly available methods for detecting phishing attacks are blacklists/whitelists, natural language processing, visual similarity, rules, machine learning techniques	Wireshark, 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