

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

Date	15 October 2022
Team ID	PNT2022TMID30811
Project Name	Project – 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

Example: Order processing during pandemics for offline mode

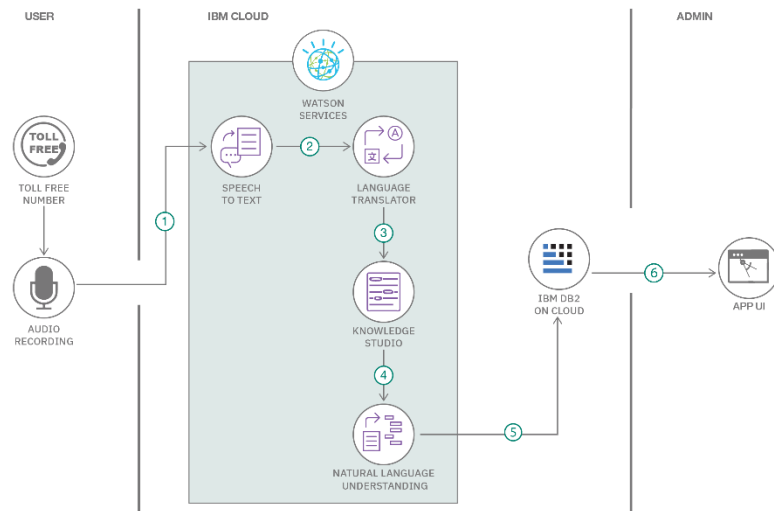


Table-1 : Components & Technologies:

Guidelines:

1. Include all the processes (As an application logic / Technology Block)
2. Provide infrastructural demarcation (Local / Cloud)
3. Indicate external interfaces (third party API's etc.)
4. Indicate Data Storage components / services
5. Indicate interface to machine learning models (if applicable)

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 Filesystem
8.	External API-1	Purpose of External API used in the application	IBM Weather API, etc.
9.	External API-2	Purpose of External API used in the application	Aadhar API, etc.
10.	Machine Learning Model	Purpose of Machine Learning Model	Object Recognition Model, etc.
11.	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 that makes it easy to test your organization's exposure to phishing.	Go phish, Speed Phish Framework (SPF), King Phisher, etc
2.	Security Implementations	It is the security discipline that makes it possible for the right entities (people or things) to use the right resources (applications or data) when they need to, without interference, using the devices they want to use.	e. g, anti-phishing protection and antispam software et
3.	Scalable Architecture	Compose is a tool for defining and running multi container Docker applications. With a single command, can create and start all the services from the configuration.	Response time, Throughput, CPU and network usages, etc.
4.	Availability	It can balance the load traffic among the servers to help improve uptime. Can scale applications by adding or removing servers, with minimal disruption to traffic flows.	IBM Cloud load balancers
5.	Performance	It provides performance feedback such as page size and how long it takes to load a page, and can show the impact new features have on the performance of the site.	Blacklists/whitelists, Natural language Processing, Visual similarity, rules, machine learning techniques, etc