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

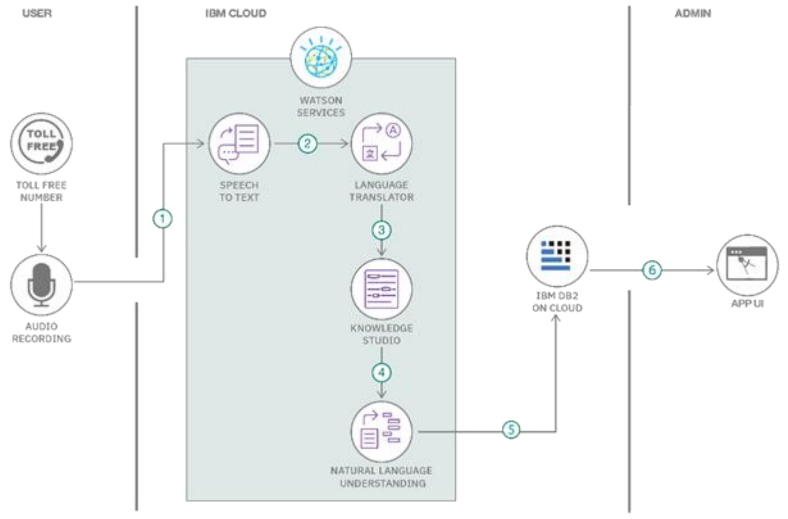
Date	27 October 2023
Team ID	PNT2022TMIDxxxxxx
Project Name	Project – 6 (AI-Driven Incident Response Platform That Assists Cybersecurity Teams in Automating Incident Triage and Response Tasks.)
Maximum Marks	4 Marks

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

Reference: https://developer.ibm.com/patterns/ai-powered-backend-system-for-order-processing-during-pandemics/



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)

Table 1 - Components & Technologies:

S.No	Component	Description	Technology
1.	Incident Triage and Response System	Central component managing incident response	Programming Languages: Python, Java
2.	User Authentication and Authorization	Handles user authentication and authorization	Java / Python
3.	Incident Triage	Responsible for receiving and storing incidents	Programming Languages: Python, Java
4.	AI Analysis Engine	Analyses incidents using AI algorithms and rules	Machine Learning / AI: TensorFlow, Scikit-Learn
5.	Incident Classification and Prioritization	Classifies and prioritizes incidents	Programming Languages: Python, Java
6.	Incident Response Automation	Executes automated response actions	Programming Languages: Python, Java
7.	Notification Service	Sends notifications to users and stakeholders	Programming Languages: Python, Java
8.	Logging and Auditing	Records system activities for auditing	Data Storage: SQL Database (e.g., MySQL)
9.	Administrator	Component for system administrators	Programming Languages: Python, Java
10.	External Systems	Interfaces with external security systems	External API Integration: RESTful APIs
11.	Reporting System	Generates and transmits incident reports	Programming Languages: Python, Java

Table 2 - Application Characteristics:

S.No	Characteristics	Description	Technology
1.	Scalability	Ability to scale based on incident volume	Cloud Computing, Load Balancing
2.	Security	Implementation of security measures	Encryption, Authentication
3.	Real-time	Capability to respond to incidents in real-time	Real-time Data Processing
4.	Accessibility	Accessible from various devices and locations	Web-Based Interface
5.	Usability	User-friendly and intuitive interface	User Experience (UX) Design
6.	Performance	High performance to handle incident data	Optimization, Caching
7.	Reliability	Ensuring minimal downtime and system reliability	Redundancy, Failover
8.	Integration	Ability to integrate with external systems	API Integration, Data Exchange
9.	Reporting	Generation of detailed incident reports	Reporting Tools, Data Visualization
10.	Compliance	Adherence to relevant cybersecurity regulations	Compliance Frameworks, Auditing