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

|  |  |
| --- | --- |
| Date | 029 October 2023 |
| Team ID | Team-591481 |
| Project Name | Advesarial attack and defences |
| Maximum Marks | 4 Marks |

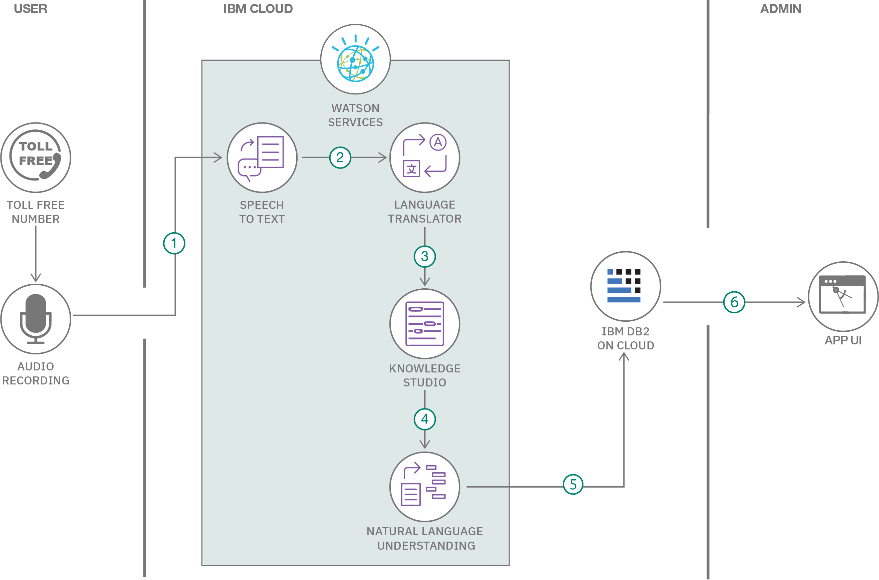


Table-1 : Components & Technologies:

**S No | Description | Technology**

**1 | User Interface | HTML, CSS, JavaScript / Angular JS / React JS**

**2 | Application Logic 1 | Python / TensorFlow / PyTorch**

**3 | Application Logic 2 | Python / ART / CleverHans / Foolbox**

**4 | Database | MongoDB / MySQL / PostgreSQL**

**5 | Machine Learning Model | CNN / RNN / GAN / BERT**

**6 | Attack | FGSM / PGD / CW / ZOO**

**7 | Defense | Adversarial Training / Defensive Distillation / Feature Squeezing / Certified Robustness**

**8 | Evaluation Metrics | Accuracy/Robustness / Privacy / Fairness**

**9 | Tools | Matplotlib / Seaborn / Plotly**

**10 | Deployment Platform | AWS / Azure / Google Cloud**

**11 | Monitoring Tools | TensorBoard / MLflow / Prometheus**

**Table 2: Characteristics**

**S No | Description | Technology**

**1 | Scalability | Horizontal / Vertical**

**2 | Availability | High / Low**

**3 | Security | Encryption / Authentication / Authorization**

References:

<https://c4model.com/>

<https://developer.ibm.com/patterns/online-order-processing-system-during-pandemic/> <https://www.ibm.com/cloud/architecture>

<https://aws.amazon.com/architecture>

<https://medium.com/the-internal-startup/how-to-draw-useful-technical-architecture-diagrams-2d20c9fda90d>