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

Date	24 October 2023
Team ID	Team-593456
Project Name	Project - Adversarial attacks and Defenses
Maximum Marks	4 Marks

TECHNOLOGY STACK FOR ADVERSARIAL ATTACKS AND DEFENSES :

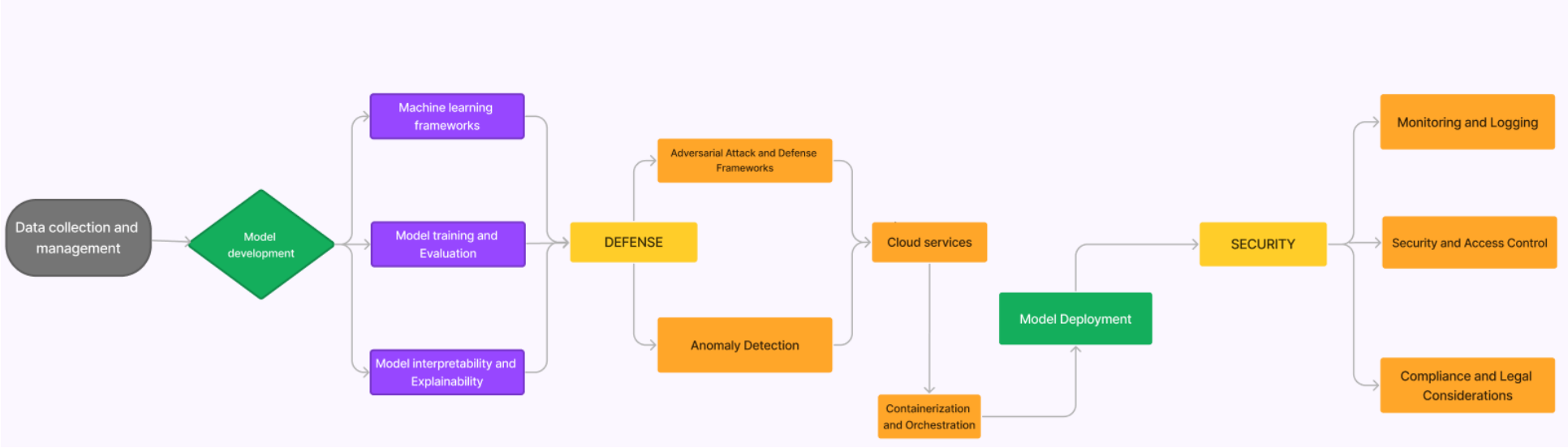

Table-1 : Components & Technologies:

S.No	Component	Description	Technology
1.	User Interface	Any app that uses AI to answer the questions and requires constant updates to stay accurate and up-to-date with information	HTML, CSS, JavaScript / Angular Js / React Js etc.
2.	Data collection and Management	Data collection, preprocessing, and labeling tools,Options to upload and manage datasets,Visualizations of data distribution	Websites,APIs,Scrapy,Python libraries ,OpenRefine etc.
3.	Model training and evaluation	Use tools for evaluating model robustness and security,Metrics for assessing model performance under adversarial conditions	TensorFlow,PyTorch,JupyterNotebooks, keras,XGBoost and LightGBM etc.
4.	Defense mechanisms	Use defense frameworks like input preprocessing, gradient masking,feature engineering and anomaly detection techniques to act quickly	Numpy,scikit-learn,federated learning frameworks like TensorFlow Federated, PySyft and IDS like SIEM etc.
5.	Database	It is a structured collection of data that is organized and stored in a way that allows for efficient data retrieval and management.It contains all types of data.	MySQL, NoSQL, etc.
6.	Cloud Database	Plays a crucial role offering scalability, flexibility, and resources for deploying, managing, and securing machine learning models and other components.	AWS, Google Cloud, Azure,Oracle cloud,IBM Cloud,GCP etc.
7.	File Storage	File storage is an important aspect and especially when it comes to managing datasets, model checkpoints, and other essential files and inculcated by many applications and corporations.	AWS S3, Azure Blob Storage, Google Cloud Storage etc.
8.	Monitoring and Logging	The combination of real-time monitoring and thorough logging provides organizations with the tools and insights needed to proactively defend against threats and respond to security incidents effectively.	IBM QRadar,Elastic SIEM,Graylog, Logstash,Wireshark,SentinelOne,AWS CloudWatch etc.
9.	Access control	Access control is a fundamental security measure that is crucial.It helps protect systems and data by ensuring that only authorized individuals or processes can access resources.	MFA,RBAC,Access control lists,WAFs,Privileged access management,Network access control etc.
10.	Machine Learning Model	To enhance the resilience of the systems by detecting or mitigating adversarial inputs, ensuring their robustness and accuracy in the face of potential threats.	Adversarial training,Feature squeezing,Robust optimization,Secure aggregation etc.
11.	Infrastructure (Server / Cloud)	Should be taken depending upon the specific needs of your application, budget constraints, scalability requirements, and your team's expertise.	AWS,Azure,CDNs,Container orchestration,On-premises data centers etc.

Table 2: Application Characteristics:

S.No	Characteristics	Description	Technology
1.	Open-Source Frameworks	Valuable in building AI filters for detecting and mitigating adversarial attacks in the context of machine learning and cybersecurity. Provide a starting point for developing robust defenses against adversarial threats.	CleverHans,Adversarial Robustness Toolbox (ART),IBM Adversarial Robustness 360 (ART 360) etc.
2.	Security Implementations	Adversarial Training,Robust Model Architectures, Adaptive Learning Rates,Regular Security Audits and so on.	IDS,Firewalls,WAFs,Access control systems, Deception technologies, etc.
3.	Scalable Architecture	An event-driven model such that each component subscribes to relevant events and takes appropriate action. It offers real-time responsiveness and scalability by adding event handlers as needed.	Apache Kafka,Apache Cassandra,AWS Lambda,Kubernetes,Spring Cloud Stream etc.
4.	Availability	Using load balancing to distribute incoming network traffic across multiple AI filter instances or servers,CDNs,Auto-Scaling to ensure the availability.	NGINX,Kubernetes,Cloudflare,AWS Auto Scaling,Squid etc.
5.	Performance	Design considerations include scalability, caching, CDNs, efficient algorithms, rate limiting and so on to ensure the system can handle high request volumes while maintaining a responsive user experience and effective defense.	NGINX, HAProxy, Redis ,Akamai,Apache Kafka,Cloudflare etc.