Project Planning Phase

Technology Stack (Architecture & Stack)

Date: 30 April 2025

Project Name: AI-Based Threat Intelligence Platform

Maximum Marks: 4 Marks

Technical Architecture

The proposed solution is an AI-powered cyber threat intelligence platform designed to monitor, detect, and respond to cyber threats in real-time. It includes multiple layers such as data ingestion, AI-based analysis, alert generation, and user dashboards. The platform integrates with third-party tools and leverages cloud-based infrastructure for scalability and availability.

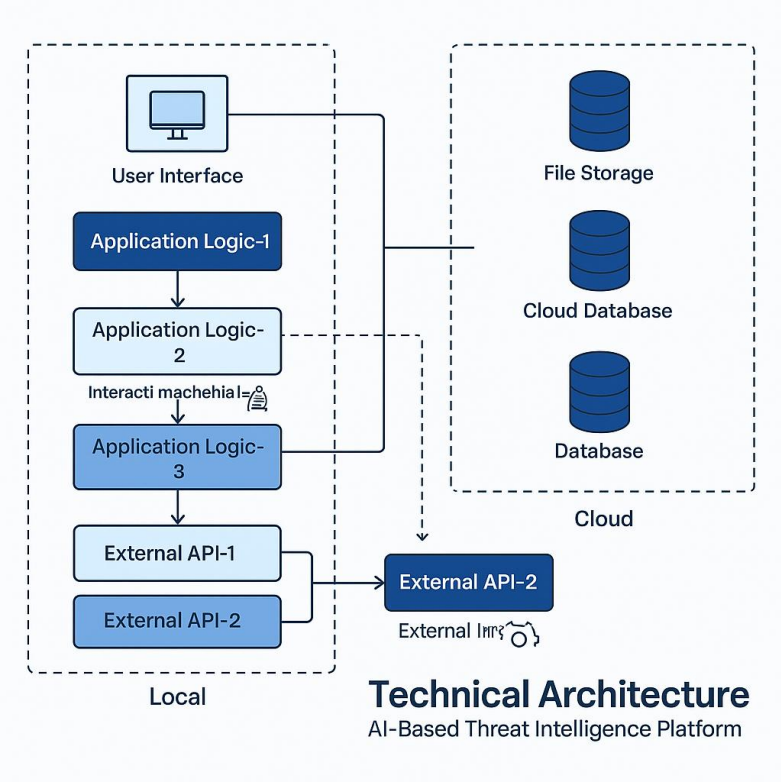

Table-1: Components & Technologies

S.NO	Component	Description	Technology
1	User Interface	Web UI for security analysts	HTML, CSS, JavaScript, Streamlit
2	Application Logic-1	Threat detection logic	Python, Pandas, Scikit-learn
3	Application Logic-2	Data aggregation and preprocessing	Python
4	Application Logic-3	Alert generation and risk scoring	Python
5	Database	Stores historical threat data	MongoDB (NoSQL)
6	Cloud Database	Cloud-based data persistence	MongoDB Atlas
7	File Storage	Logs and model files	AWS S3 / Local Filesystem
8	External API-1	Threat intelligence feeds	VirusTotal API, AbuseIPDB API
9	External API-2	Log analysis and enrichment	Shodan API
10	Machine Learning Model	Detects anomalies and classifies threats	Isolation Forest, Logistic Regression
11	Infrastructure	Cloud server for hosting the application	AWS EC2 / Kubernetes

Table-2: Application Characteristics

S.No	Characteristics	Description	Technology / Approach
1	Open-Source Frameworks	Frameworks and libraries used	Scikit-learn, Flask, Streamlit
2	Security Implementations	Securing endpoints and data	HTTPS, Token-based Auth, IAM, Firewalls
3	Scalable Architecture	Can be scaled horizontally using containerized services	Docker, Kubernetes, Microservices
4	Availability	High availability through distributed setup	AWS Load Balancer, Multi-Zone Hosting
5	Performance	Optimized performance for real-time alerts	Redis Cache, CDN, Async Processing

---

References:

- https://aws.amazon.com/architecture
- https://cloud.google.com/architecture
- https://www.ibm.com/cloud/architecture
- https://c4model.com/