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.

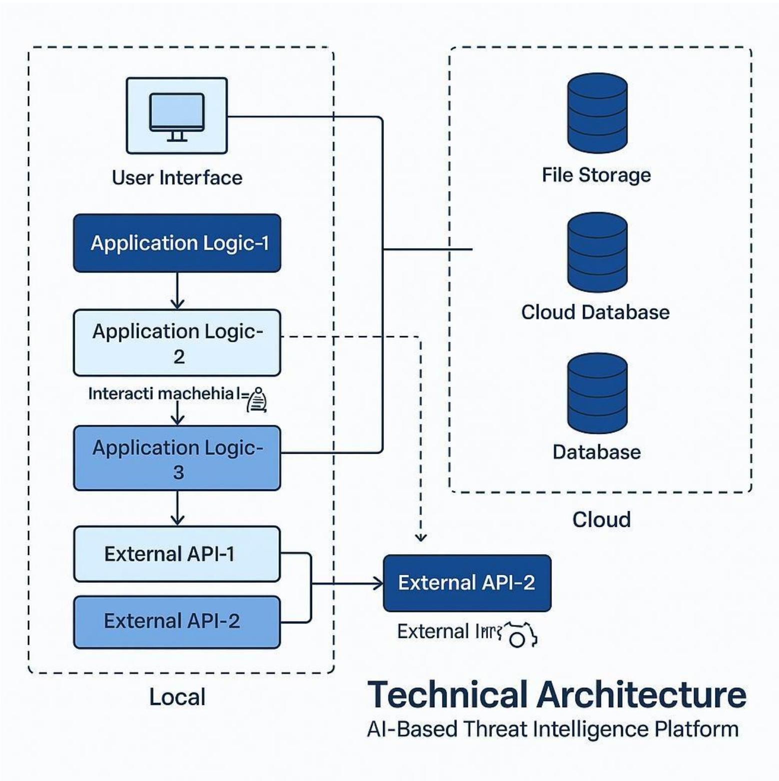

Table-1: Components & Technologies

S.NO	**Component**	**Description**	**Technology**
1	User Interface	Not implemented (CLI-based only)	N/A *(No UI implemented)*
2	Application Logic-1	IP reputation analysis using ML classifier	Python, Scikit-learn, Random Forest Classifier
3	Application Logic-2	Data preprocessing (encoding, feature extraction)	Python, Pandas, LabelEncoder
4	Application Logic-3	Threat prediction and classification logging	Python, Logging module
5	Database	Not used; processed data stored in local files	Local Filesystem (Pickle, CSV)
6	Cloud Database	Not implemented	N/A
7	File Storage	stores logs, models, encoders, dataset	Local Filesystem (.pkl, .csv)
8	External API-1	Fetches IP reputation data	AbuseIPDB API
9	External API-2	Not used	N/A
10	Machine Learning Model	Classifies IPs as malicious or benign	Random Forest Classifier
11	Infrastructure	Local execution using Python scripts	Local Machine (Windows environment)

Table-2: Application Characteristics

S.No	Characteristics	Description	Technology / Approach
1	Open-Source Frameworks	Frameworks and libraries used	Scikit-learn, Pandas, Joblib
2	Security Implementations	Not applicable at current phase (ofline only)	N/A
3	Scalable Architecture	Modular structure allows for cloud integration and automation later	Python modules with expandable structure
4	Availability	Executed manually via scripts; not hosted or deployed	Ofline local execution
5	Performance	Fast predictions on structured input; real-time not supported yet	Lightweight models and efficient preprocessing