Project Design Phase-II

Technology Stack (Architecture & Stack)

Technical Architecture:

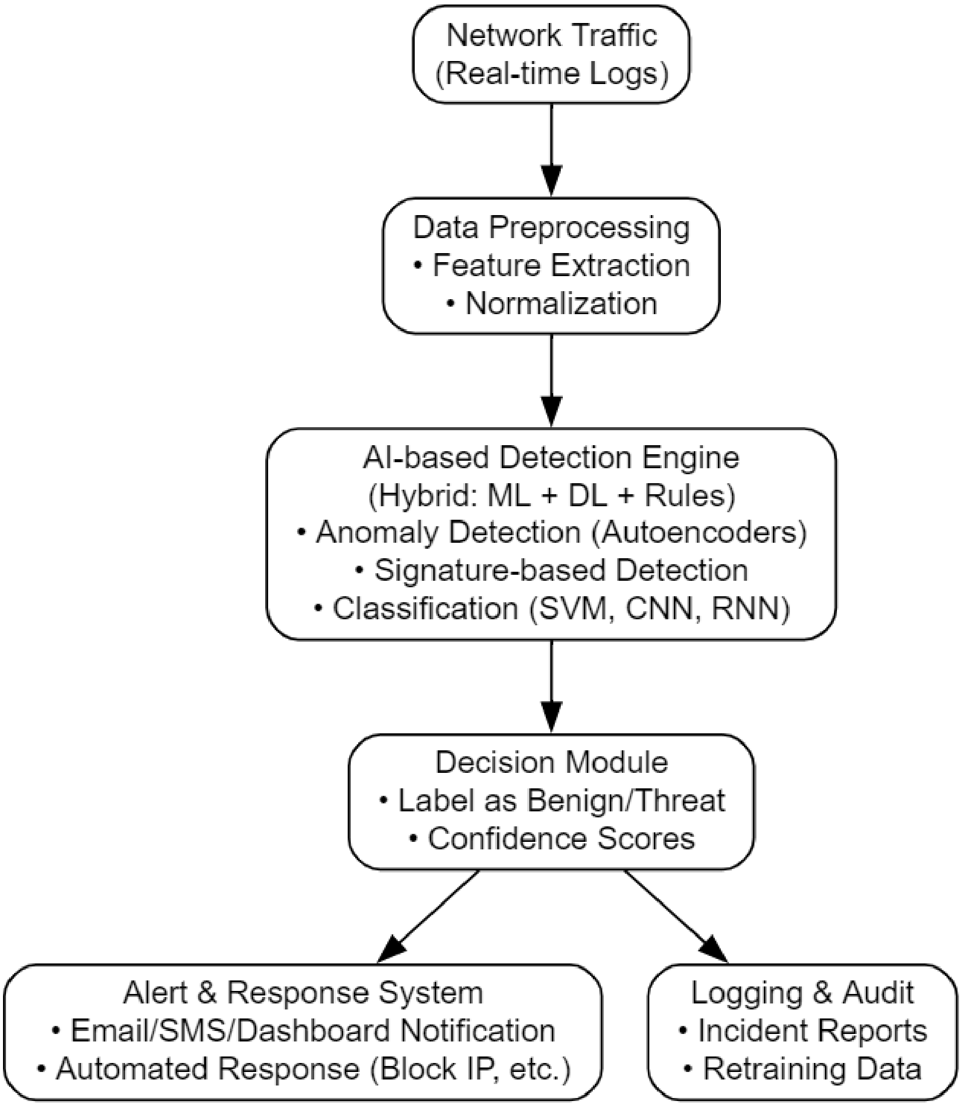

Table-1 : Components & Technologies:

S.No	Component	Description	Technology
1	Data Collection	Captures real-time network traffic and logs for analysis	Packet Sniffer (e.g., Wireshark), TCPDump
2	Data Preprocessing	Cleans and transforms data into usable format for AI models	Python (Pandas, Scikit-learn)
3	Feature Extraction	Identifies relevant attributes from network data (e.g., duration, bytes)	Scikit-learn, Manual heuristics
4	AI Detection Engine	Detects anomalies or known attack patterns using machine learning	Random Forest / SVM / Neural Networks
5	Alert Generation Module	Triggers real-time alerts for suspicious behavior	Flask / Django + Notification APIs
6	Logging & Reporting	Maintains logs and generates summaries for admins	Logstash / ELK Stack
7	Model Training Module	Trains and updates models with new attack data	Python, Jupyter Notebooks
8	Threat Intelligence Feed	Optional external feed to keep model updated with latest threats	Threat Intelligence APIs

Table-2: Application Characteristics:

S.No	Characteristics	Description	Technology / Approach
1	Real-time Detection	Identifies intrusions as they happen	Streaming + AI classification
2	High Accuracy	Improves precision in classifying threats vs normal traffic	Random Forest / XGBoost
3	Reduced False Positives	Uses AI to better distinguish between benign anomalies and actual attacks	Supervised Learning Models
4	Scalable	Can be expanded for large-scale networks	Cloud-native / Containerized
5	Adaptive Learning	Learns from new attack vectors over time	Online Learning / Reinforcement Learning
6	Multi-Attack Detection	Detects DoS, Probe, R2L, and U2R attacks	NSL-KDD Dataset Training
7	Explainability	Provides insight into why an alert was triggered	SHAP / LIME
8	Integration Capability	Can be plugged into existing network infrastructure	APIs / Webhooks