Model Research Document

Development of Interactive Cyber Threat Visualization Dashboard

1. Introduction

Cybersecurity environments generate massive volumes of security incident data from sources such as CVE feeds, system logs, and simulated attack records. Manual analysis of this data is time-consuming and error-prone. This project integrates Artificial Intelligence (AI) and Machine Learning (ML) models with an interactive visualization dashboard to provide real-time insights into cyber threats, enabling proactive risk mitigation and improved security posture.

2. Purpose of Using AI & ML in the Project

• Detect known and unknown cyber threats

• Identify anomalies and unusual attack behavior

• Analyze time-based attack trends

• Prioritize vulnerabilities and affected systems

• Enhance executive-level security reporting

The outputs of these models are visualized using Plotly/Dash to support fast and informed decision-making.

3. Machine Learning & AI Models Used (10+ Models)

1. Logistic Regression

Type: Supervised ML

Purpose: Threat severity classification

Application: Classifies security incidents into low, medium, and high-risk categories.

Dashboard Usage: Severity distribution graphs and risk-level filters.

2. Naive Bayes

Type: Supervised ML (NLP-based)

Purpose: Text-based threat classification

Application: Analyzes CVE descriptions and security logs to identify attack types such as phishing or malware.

Dashboard Usage: Attack-type charts and MITRE ATT&CK; categorization.

3. Decision Tree

Type: Supervised ML

Purpose: Rule-based threat detection

Application: Identifies intrusion patterns using human-readable decision rules.

Dashboard Usage: Explainable threat paths and root cause analysis.

4. Random Forest

Type: Ensemble ML

Purpose: High-accuracy threat detection

Application: Improves detection accuracy for malware and intrusion attacks.

Dashboard Usage: Threat confidence scores and prioritized vulnerability lists.

5. Support Vector Machine (SVM)

Type: Supervised ML

Purpose: Complex attack classification

Application: Detects threats in high-dimensional network traffic data.

Dashboard Usage: Precision-based detection metrics and comparisons.

6. K-Means Clustering

Type: Unsupervised ML

Purpose: Geographical and behavioral clustering

Application: Groups attack sources and targets to identify cyber risk hotspots.

Dashboard Usage: Geospatial risk maps and heatmaps.

7. Isolation Forest

Type: Unsupervised ML

Purpose: Anomaly detection

Application: Detects abnormal spikes and zero-day attack behavior.

Dashboard Usage: Time-series anomaly indicators and alerts.

8. Autoencoders

Type: Deep Learning

Purpose: Unknown and zero-day threat detection

Application: Learns normal system behavior and flags deviations.

Dashboard Usage: Anomaly scores and risk intensity visualizations.

9. Long Short-Term Memory (LSTM)

Type: Deep Learning (RNN)

Purpose: Sequential attack detection

Application: Identifies slow and multi-stage cyber attacks over time.

Dashboard Usage: Attack progression timelines and behavioral analysis charts.

10. ARIMA / Facebook Prophet

Type: Time-Series Forecasting

Purpose: Attack trend prediction

Application: Forecasts future attack frequency and seasonal patterns.

Dashboard Usage: Trend forecast charts and future risk indicators.

11. BERT / CyberBERT

Type: Transformer-based AI

Purpose: Threat intelligence analysis

Application: Analyzes detailed CVE reports and threat intelligence documents.

Dashboard Usage: Executive summaries and keyword-based threat insights.

4. Model Integration with Project Modules

Project Module	Objective	ML / AI Models Used
Module 1	Data acquisition & structuring	Naive Bayes, Logistic Regression
Module 2	Trend & anomaly detection	Isolation Forest, ARIMA
Module 3	Geospatial & vulnerability analysis	K-Means, Decision Tree
Module 4	Dashboard integration & intelligence	Random Forest, Autoencoder, LSTM

5. Alignment with Project Outcomes

• Geospatial Risk Mapping: K-Means, Random Forest

• Trend & Anomaly Detection: Isolation Forest, LSTM, ARIMA

• Vulnerability Prioritization: Decision Tree, Random Forest

• Enhanced Reporting: Logistic Regression, BERT

6. Conclusion

The integration of 10+ AI and ML models enhances the Interactive Cyber Threat Visualization Dashboard by transforming raw security data into actionable intelligence. These models enable effective threat detection, anomaly identification, trend forecasting, and vulnerability prioritization. Combined with interactive visualizations, the system supports proactive cybersecurity decision-making and strengthens the overall security posture of an organization.