Model Study: ML & DL Techniques for Cyber Threat Visualization Dashboard

1. Introduction

A cyber threat visualization dashboard is designed to monitor, detect, and analyze security threats using intelligent techniques. Machine Learning (ML) and Deep Learning (DL) models play a key role in identifying malicious activities, abnormal patterns, and attack severity from large volumes of network and system data. These results are then represented visually to assist security analysts in decision-making.

2. Machine Learning Techniques

2.1 Logistic Regression

Category: Supervised Learning
Application: Classification of network traffic as normal or malicious
Benefits: Easy to implement, fast execution, interpretable results
Drawback: Limited performance for complex attack patterns

2.2 Decision Tree

Category: Supervised Learning
Application: Intrusion detection using rule-based decisions
Benefits: Simple logic, easy to understand and visualize
Drawback: Can overfit the training data

2.3 Random Forest

Category: Ensemble Learning
Application: Detection of intrusions and anomalies
Benefits: High accuracy and robust performance
Drawback: Reduced transparency compared to single models

2.4 Support Vector Machine (SVM)

Category: Supervised Learning
Application: Classification of high-dimensional cyber threats
Benefits: Effective in defining clear decision boundaries
Drawback: High computational requirements

2.5 K-Nearest Neighbors (KNN)

Category: Instance-Based Learning
Application: Detection based on similarity between data points
Benefits: Simple and intuitive approach
Drawback: Performance degrades with large datasets

3. Deep Learning Techniques

3.1 Artificial Neural Network (ANN)

Application: Multi-category cyber attack classification
Advantage: Capable of learning complex relationships in data

3.2 Convolutional Neural Network (CNN)

Application: Extraction of features from network traffic data
Advantage: Improved detection accuracy for structured inputs

3.3 Recurrent Neural Network (RNN)

Application: Analysis of sequential network activities
Advantage: Suitable for time-based threat detection

3.4 Long Short-Term Memory (LSTM)

Application: Monitoring and forecasting network traffic behavior
Advantage: Handles long-term dependencies effectively

3.5 Autoencoders

Application: Detection of anomalies and unknown attacks
Advantage: Works without labeled data using unsupervised learning

4. Summary

Both Machine Learning and Deep Learning models provide effective solutions for cyber threat detection. Choosing the appropriate model based on data type and system requirements enhances the accuracy and efficiency of cyber threat visualization dashboards.