Model Research: ML/DL Models for Cyber Threat Visualization Dashboard

1. Overview

Cyber threat visualization dashboards rely on intelligent models to detect, classify, and analyze malicious activities from network and system data. Machine Learning (ML) and Deep Learning (DL) models help identify attack patterns, anomalies, and threat severity, which are then visualized interactively for security analysts.

2. Machine Learning Models

2.1 Logistic Regression
Type: Supervised ML
Use Case: Binary classification (attack vs normal)
Advantages: Simple, fast, interpretable
Limitation: Not suitable for complex attacks

2.2 Decision Tree
Type: Supervised ML
Use Case: Rule-based intrusion detection
Advantages: Explainable, easy to visualize
Limitation: Overfitting

2.3 Random Forest
Type: Ensemble ML
Use Case: Intrusion and anomaly detection
Advantages: High accuracy, scalable
Limitation: Less interpretability

2.4 Support Vector Machine (SVM)
Type: Supervised ML
Use Case: High-dimensional attack classification
Advantages: Effective decision boundaries
Limitation: Computational cost

2.5 K-Nearest Neighbors (KNN)
Type: Instance-based ML
Use Case: Similarity-based detection
Advantages: Simple implementation
Limitation: Slow on large datasets

3. Deep Learning Models

3.1 Artificial Neural Network (ANN)
Use Case: Multi-class attack classification
Strength: Learns complex patterns

3.2 Convolutional Neural Network (CNN)
Use Case: Network traffic feature extraction
Strength: High detection accuracy

3.3 Recurrent Neural Network (RNN)
Use Case: Sequential traffic analysis
Strength: Time-based detection

3.4 Long Short-Term Memory (LSTM)
Use Case: Traffic monitoring and prediction
Strength: Handles long-term dependencies

3.5 Autoencoders
Use Case: Anomaly and zero-day attack detection
Strength: Unsupervised learning

4. Conclusion
Different ML and DL models offer varied strengths in cyber threat detection. Selecting suitable models improves the effectiveness of interactive cyber threat visualization dashboards.