MODEL RESEARCH

Title: Research Review on Single ML/DL Models for Cyber Attack Detection

Internship Program: Infosys Springboard Internship
Project Title: Cyber Attack Detection Using Machine Learning / Deep Learning
Intern Name: Rajitha Reddy

Introduction

This document presents a focused research review of ten cybersecurity research papers. Each paper uses only one Machine Learning (ML) or Deep Learning (DL) model for cyber attack detection. The review follows a structured order including the prompt used, model selected, reason for model usage, accuracy achieved during training/testing, and the research paper link.

Paper 1: Random Forest for Intrusion Detection

Prompt Used: Find a research paper using Random Forest for intrusion detection in networks.

Model Used: Random Forest (Machine Learning)

Why is it Used: Random Forest is used because it provides high accuracy, handles large datasets, and reduces overfitting.

Accuracy of Model: Achieved up to 99.8% accuracy during training and testing.

Paper Link: https://www.mdpi.com/2076-3417/15/4/1903

Paper 2: XGBoost for Anomaly-Based Intrusion Detection

Prompt Used: Find a research paper that uses XGBoost for anomaly-based intrusion detection.

Model Used: XGBoost (Machine Learning)

Why is it Used: XGBoost is used for its fast training and ability to handle complex feature interactions.

Accuracy of Model: Achieved nearly 100% accuracy during experimental testing.

Paper Link: https://www.frontiersin.org/articles/10.3389/frai.2025.1625891

Paper 3: Random Forest for Signature-Based Intrusion Detection

Prompt Used: Find a research paper using Random Forest for signature-based cyber attack detection.

Model Used: Random Forest (Machine Learning)

Why is it Used: It is effective in identifying known attack patterns with high reliability.

Accuracy of Model: Achieved approximately 99.5% accuracy during testing.

Paper Link: https://www.nature.com/articles/s41598-025-85866-7

Paper 4: CNN for IoT Intrusion Detection

Prompt Used: Find a research paper using CNN for intrusion detection in IoT networks.

Model Used: Convolutional Neural Network – CNN (Deep Learning)

Why is it Used: CNN is used to capture spatial features from IoT network traffic.

Accuracy of Model: Achieved around 98.42% accuracy after training and testing.

Paper Link: https://arxiv.org/abs/2405.18624

Paper 5: 1D CNN for IoT Network Security

Prompt Used: Find a research paper using 1D CNN for real-time IoT intrusion detection.

Model Used: 1D Convolutional Neural Network (Deep Learning)

Why is it Used: 1D CNN is lightweight and suitable for real-time detection with low computation cost.

Accuracy of Model: Achieved approximately 99.5% accuracy during testing.

Paper Link: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-025-00202-w

Paper 6: KNN for Cyber Attack Classification

Prompt Used: Find a research paper using KNN for cyber attack detection.

Model Used: K-Nearest Neighbors – KNN (Machine Learning)

Why is it Used: KNN is used for its effectiveness in multiclass classification problems.

Accuracy of Model: Achieved up to 99.83% accuracy in testing phase.

Paper Link: https://arxiv.org/abs/2105.13435

Paper 7: ANN for Cyber Threat Detection

Prompt Used: Find a research paper using Artificial Neural Networks for cyber threat detection.

Model Used: Artificial Neural Network – ANN (Deep Learning)

Why is it Used: ANN is used to learn complex patterns and reduce false positives.

Accuracy of Model: Achieved higher accuracy than traditional ML models during testing.

Paper Link: https://www.ijraset.com/research-paper/cyber-threat-detection-based-on-artificial-neural-networks

Paper 8: Random Forest for Cloud Anomaly Detection

Prompt Used: Find a research paper using Random Forest for anomaly detection in cloud environments.

Model Used: Random Forest (Machine Learning)

Why is it Used: It provides stable performance and high detection accuracy in cloud data.

Accuracy of Model: Detection accuracy exceeded 99% during testing.

Paper Link: https://arxiv.org/abs/1812.05443

Paper 9: CNN for Anomaly-Based Intrusion Detection

Prompt Used: Find a research paper using CNN for anomaly-based intrusion detection.

Model Used: Convolutional Neural Network – CNN (Deep Learning)

Why is it Used: CNN reduces false positives and improves anomaly detection.

Accuracy of Model: Achieved approximately 99.87% accuracy during testing.

Paper Link: https://www.nature.com/articles/s41598-025-08175-z

Paper 10: LSTM for Network Traffic Monitoring

Prompt Used: Find a research paper using LSTM for cyber attack detection and traffic monitoring.

Model Used: Long Short-Term Memory – LSTM (Deep Learning)

Why is it Used: LSTM is used to analyze sequential and time-series network traffic data.

Accuracy of Model: Accuracy ranged between 82% and 99% after training and testing.

Paper Link: https://www.mdpi.com/2078-2489/15/11/741