AI /ML Models for Cyber Threat Analysis

A Research Study for an Interactive Cyber Threat Visualization Dashboard

Model Research Document

Project: Development of Interactive Cyber Threat Visualization Dashboard

Prepared By

Joshitha Mugunthan

TABLE OF CONTENT

Abstract

Cyber threat analysis requires processing vast, heterogeneous data in real time. Modern networks generate “billions of data” from servers, firewalls, IDS/IPS and devices. Traditional signature-based detection cannot adapt to new or evolving attacks, so analysts increasingly rely on AI/ML techniques. These models learn normal traffic patterns and flag anomalies or attack signatures automatically. For example, ML-driven intrusion detection systems can monitor network flows continuously, build time-series baselines of normal behavior, and immediately alert on any abnormal spike or pattern. In this context, we review ten leading AI/ML models used for threat analysis, describing their workings, prediction abilities, live-stream use, APIs, and global impact. At the end, one model is highlighted as especially well-suited to a real-time threat visualization dashboard.

Introduction To Cyber Threat Analysis

Modern organizations operate highly connected digital infrastructures that are continuously exposed to cyber threats. The rapid growth of networked devices, cloud platforms, and online services has expanded the attack surface. Cyber threat analysis focuses on identifying malicious activities, understanding attack patterns, and mitigating risks before they escalate into large-scale incidents. With attackers constantly evolving techniques, static rule-based security mechanisms are no longer sufficient, motivating the shift toward intelligent, adaptive analytical approaches.

Role of AI and Machine Learning in Cybersecurity

AI and Machine Learning models enable automated analysis of massive security datasets that are impossible to process manually. These models learn baseline behavior, detect deviations, classify attacks, and predict future threats. By continuously monitoring live network traffic and logs, ML-driven systems can identify subtle anomalies, reduce false positives, and improve detection speed. As a result, AI-driven cybersecurity systems support proactive defense, real-time alerting, and strategic decision-making at both organizational and global levels.

Data Sources for AI-Driven Cyber Threat Analysis

AI/ML models for cyber threat analysis rely on diverse data sources, including network traffic flows, firewall logs, IDS/IPS alerts, endpoint telemetry, authentication logs, vulnerability databases, and threat intelligence feeds. These heterogeneous datasets provide information about protocols, packet behavior, user actions, system events, and known vulnerabilities. When aggregated and normalized, such data enables accurate modeling of normal behavior and detection of abnormal or malicious activities in real time.

AI/ML Models for Cyber Threat Analysis

1. Decision Trees and Random Forests

Decision Trees are simple, tree-like classifiers that split network data (features like packet rates, protocols, etc.) by thresholds to separate “safe” vs. “malicious” traffic. Their main advantage is interpretability – one can trace the decision path. Random Forests are ensembles of decision trees: many trees are built on random feature subsets and their votes combined. This reduces overfitting and boosts

accuracy. In cyber analysis, Random Forests have been widely applied for intrusion detection. These models can be deployed via tools like scikit-learn or cloud ML services to score live network flows as they arrive.

2. *Support Vector Machines (SVM)*

Support Vector Machines are supervised classifiers that find an optimal hyperplane to separate classes with maximum margin. In cybersecurity, SVMs have been used to distinguish malicious patterns such as DoS attacks or scanning behavior. One-Class SVMs define a boundary of normality and flag anomalies. While accurate, SVMs can be computationally expensive for very large or streaming datasets and require careful tuning.

3. *k-Nearest Neighbors (kNN)*

k-Nearest Neighbors is an instance-based method where new samples are classified based on similarity to historical data. In cybersecurity, KNN is often used for anomaly detection by measuring distance from known normal clusters. Although simple and transparent, its real-time applicability is limited by scalability challenges unless optimized indexing techniques are used.

4. *Naïve Bayes*

Naive Bayes is a probabilistic classifier based on Bayes' theorem and an independence assumption among features. In cybersecurity, it is used for spam detection, phishing classification, and baseline intrusion filtering. Its main advantages are speed, scalability, and ease of incremental updates, though its accuracy may be lower compared to ensemble models.

5. *k-Means Clustering*

k-Means is an unsupervised clustering algorithm that groups similar network behaviors into clusters. It helps identify traffic modes and outlier behavior without labeled data. Mini-batch k-means allows adaptation to streaming environments, making it useful for exploratory analysis and anomaly grouping in large-scale networks.

6. *Isolation Forest (Anomaly Detection)*

Isolation Forest is an unsupervised anomaly detection model that isolates anomalies through random partitioning. Rare or unusual events are detected efficiently and assigned high anomaly scores. It is well-suited for zero-day threat detection and is commonly integrated into security platforms for real-time anomaly scoring.

7. *Autoencoders (Deep Anomaly Detection)*

Autoencoders are neural networks trained to reconstruct normal network traffic. High reconstruction error indicates anomalies. This makes autoencoders highly effective for detecting unknown or evolving threats in live environments. They can be deployed using modern ML frameworks and are used in industry systems such as encrypted traffic analysis tools.

8. Neural Networks (CNN, RNN, LSTM)

Deep Neural Networks such as CNNs and RNNs/LSTMs learn complex spatial and temporal patterns in cyber data. CNNs detect localized patterns, while LSTMs model sequential behavior and temporal dependencies. These models

enable detection of multi-step attacks and forecasting of attack trends but require large datasets and significant computational resources.

9. Graph Neural Networks (GNN)

Graph Neural Networks model cybersecurity data as graphs, capturing relationships between hosts, flows, and events. By propagating information across nodes and edges, GNNs identify coordinated and multi-hop attacks. They are increasingly used in advanced intrusion detection research and threat intelligence correlation.

10. Transformer and Attention-Based Models

Transformer-based models use attention mechanisms to capture long-range dependencies in logs, traffic sequences, and textual threat intelligence. These models excel in analyzing complex, large-scale datasets and are applied to intrusion detection, log analysis, and cyber threat intelligence generation.

Comparative Summary of AI/ML Models

The following table provides a comparative overview of the AI/ML models discussed in this study, highlighting their learning approach, suitability for real-time analysis, and primary use cases in cyber threat detection. This comparison helps in understanding the strengths and limitations of each model when applied to live cybersecurity environments and visualization dashboards.

Model	Learning Type	Supervision Level	Real-Time Suitability	Primary Use in Cyber Threat Analysis
Decision Trees	Classical ML	Supervised	High	Interpretable classification of network traffic and intrusion detection
Random Forests	Ensemble ML	Supervised	High	Accurate intrusion detection, feature importance analysis, live traffic scoring
Support Vector Machines (SVM)	Classical ML	Supervised/ Semi-supervised	Moderate	Separation of benign and malicious traffic, anomaly boundary detection
k- Nearest Neighbors (kNN)	Instance-based ML	Supervised	Low-Moderate	Similarity-based classification and baseline anomaly detection
Naïve Bayes	Probabilistic ML	Supervised	High	Fast baseline detection for spam, phishing and simple intrusions
k-Means Clustering	Clustering	Unsupervised	Moderate	Traffic pattern grouping and outlier detection without labeled data

Isolation Forest	Ensemble ML	Unsupervised	High	Detection of rare and anomalous network events, zero-day threats
Autoencoders	Deep Learning	Unsupervised	High	Deep anomaly detection using reconstruction error on live traffic
CNN/ RNN/ LSTM	Deep Learning	Supervised	Moderate-High	Spatial and temporal pattern recognition, multi-step attack detection
Graph Neural Networks (GNN)	Deep Learning	Supervised/ Semi-supervised	Moderate	Detection of coordinated and multi-hop attacks using network graphs
Transformer Models	Deep Learning	Supervised/ Semi-supervised	Moderate	Long-sequence analysis of logs, traffic streams, and threat intelligence

Interpretation

This comparative analysis shows that while traditional supervised models such as Random Forests and SVMs are effective for known attack detection, unsupervised and deep learning models like Isolation Forests and Autoencoders are better suited for identifying unknown or emerging threats in real time. Advanced architectures such as GNNs and Transformers provide deeper

contextual understanding of complex attack patterns but require higher computational resources. This comparison directly supports the selection of an appropriate model for a real-time cyber threat visualization dashboard.

Global Impact of AI-Driven Cyber Threat Detection

AI-driven cyber threat detection enhances global cybersecurity by enabling early identification of emerging attacks, reducing response times, and improving situational awareness. These models help organizations and governments detect coordinated attacks, monitor global threat trends, and respond proactively to cyber incidents that can impact critical infrastructure and economic stability.

Best-Fit Model for the Interactive Cyber Threat Visualization Dashboard

For an interactive cyber-threat visualization dashboard, deep autoencoder-based anomaly detection stands out as the best fit. Autoencoders learn normal system behavior and flag deviations in real time, making them ideal for identifying unknown and emerging threats. Their ability to operate without labeled attack data aligns with real-world cybersecurity environments and supports live visualization, geospatial mapping, and trend analysis.

Conclusion and Future Scope

AI and ML models have transformed cyber threat analysis by enabling scalable, adaptive, and real-time detection of attacks. While traditional models remain useful, deep learning and graph-based approaches offer superior capability in handling complex and evolving threats. Future work may integrate hybrid

models, attention mechanisms, and large-scale threat intelligence feeds to further enhance global cyber defense systems.

References

- IBM. *Machine Learning for Anomaly Detection*. https://www.ibm.com/think/topics/machine-learning-for-anomaly-detection
- IBM. *Supervised Learning*. https://www.ibm.com/think/topics/supervised-learning
- Neumann, P. *Predictive Analysis with Machine Learning*. wp_Softrams_p1_predictive_analysis_ML.pdf
- *Autoencoder-Based Network Anomaly Detection*. arXiv. https://arxiv.org/html/2505.16650v1
- *Graph Neural Networks for Intrusion Detection Systems*. ScienceDirect. https://www.sciencedirect.com/science/article/abs/pii/S0167404824001226
- *Transformer and Large Language Models for Intrusion Detection Systems*. ScienceDirect. https://www.sciencedirect.com/science/article/abs/pii/S1566253525004208