AI-Based Cyber Security Threat Prediction

<u>**Model Research**</u>

I. Comparative Analysis of State-of-the-Art Prediction Models

The complexity of cyber threats requires specialized AI models for different prediction tasks: statistical classification, sequential behavior analysis, and relational mapping. The optimal solution is typically a hybrid architecture leveraging multiple models.

Model Category	Example Model	Core Function / Differentiation	Why Choose (Best Fit)	Typical Accuracy / F1-Score
Ensemble / Gradient Boosting	**XGBoost/LightGBM**	Uses optimized gradient boosting algorithms.Excels at rapid classification of tabular statistics; highly **explainable via SHAP**.	Chosen as the foundational **Stage 1 filter** model due to its speed, efficiency, and high accuracy for handling large volumes of enriched, structured data.	Accuracy: **98–99.5%**. F1-Score: Up to **99.2%** on intrusion detection benchmarks.
Sequential Deep Learning	**Transformer Encoder (LSTM/RNN)**	Processes **time-ordered event sequences**; uses self-attention to capture complex, long-range dependencies.	Critical for detecting multi-step campaigns, **lateral movement**, and insider threats, where the sequence of actions is key.	Accuracy/F1: High **98–99%** achievable.Hybrid models combining CNNs/LSTMs have demonstrated 99.86% accuracy for sequential threats.

Relational Deep Learning	**Graph Neural Network (GNN)**	Constructs a graph of entities (IPs, users) and interactions (edges) to model **structural relationships**.	Provides essential **multi-hop context** for detecting coordinated attacks and identifying related threat clusters across multiple assets.	Accuracy: Generally **96–97.9%** F1/Accuracy observed on relational threat detection.
Anomaly Detection (Unsupervised)	**Autoencoder / Isolation Forest**	Learns a statistical baseline of "normal" behavior. Flags deviations (high reconstruction error).	Provides a continuous monitoring **safety net** for catching **unseen threats or zero-day attacks** since it requires no malicious labels for training.	Measured via Reconstruction Error; provides essential high sensitivity against novel threats.
Traditional ML (Baseline)	**Random Forest (RF)**	Ensemble of Decision Trees. Highly stable and requires minimal hyperparameter tuning.	Suitable for establishing a robust, easily **interpretable baseline** model for initial comparison and quick deployment.	Accuracy: **97–99%**. Known for its stability and strong performance across various datasets.

II.A. Differentiation: The Hybrid Fusion System

For maximum detection accuracy and resilience, a **Multi-Stage Hybrid Fusion System** is the recommended architecture. This system combines the specialized strengths of each model family:

- **Statistical Efficiency (XGBoost/LightGBM):** Handles massive, high-velocity tabular data for rapid initial filtering (Stage 1).
- **Temporal Context (Transformer/LSTM):** Analyzes the *sequence* of actions (behavior) to spot complex, multi-step attacks (Stage 2).
- **Structural Context (GNN):** Analyzes the *relationships* between assets and users to find coordinated threat clusters (Stage 3).
- **Zero-Day Capability (Autoencoder):** Operates in parallel to flag statistically aberrant, *unseen* activity (Stage 4).

These component models feed their prediction scores (probability, sequence score, correlation score, error score) into a **Meta-Learner** (Stage 5), typically a simple classification model. This final layer weights and combines the diverse inputs to achieve a highly reliable **Unified Risk Score**, maximizing robustness against targeted evasion and noise.[14] The combined ensemble approach consistently outperforms single classifiers in intrusion detection.

Works cited

1. CIC UNSW-NB15 Augmented Dataset - University of New Brunswick, accessed October 15, 2025, https://www.unb.ca/cic/datasets/cic-unsw-nb15.html
2. Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity - MDPI, accessed October 15, 2025, https://www.mdpi.com/2076-3417/13/13/7507
3. Intrusion detection system based on machine learning using least square support vector machine - PMC, accessed October 15, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11978955/
4. Ensemble Model Based on Hybrid Deep Learning for Intrusion Detection in Smart Grid Networks - PubMed Central, accessed October 15, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10490611/
5. Threat intelligence - Microsoft Sentinel, accessed October 15, 2025, https://learn.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence
6. What Is Cyber Threat Intelligence (CTI)? - Palo Alto Networks, accessed October 15, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-cyberthreat-intelligence-cti
7. Adoption of Deep-Learning Models for Managing Threat in API Calls with Transparency Obligation Practice for Overall Resilience - PubMed Central, accessed October 15, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11314962/

8. What Is SIEM? 7 Pillars and 13 Core Features [2025 Guide] - Exabeam, accessed October 15, 2025, https://www.exabeam.com/explainers/siem/what-is-siem/
9. SIEM vs EDR: Similarities and Differences - CrowdStrike.com, accessed October 15, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/siem-vs-edr/
10. A deep learning/machine learning approach for anomaly based network intrusion detection, accessed October 15, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC12455727/
11. Systematic Review of Graph Neural Network for Malicious Attack Detection - MDPI, accessed October 15, 2025, https://www.mdpi.com/2078-2489/16/6/470
12. A deep learning/machine learning approach for anomaly based network intrusion detection - Frontiers, accessed October 15, 2025, https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1625891/pdf
13. The Role of Ensemble Learning in Strengthening Intrusion Detection Systems: A Machine Learning Perspective - ResearchGate, accessed October 15, 2025, https://www.researchgate.net/publication/384366905_The_Role_of_Ensemble_Learning_in_Strengthening_Intrusion_Detection_Systems_A_Machine_Learning_Perspective