Selection and Evaluation of Machine Learning Models for Predictive Cyber Threat Detection

1. Executive Summary

This report researches and evaluates at least 10 AI/ML models suitable for threat prediction in an interactive cyber threat visualization dashboard. The dashboard requires a model capable of accurate, real-time or near-real-time prediction of cyber threats (e.g., intrusions, anomalies, malware) from network traffic, logs, and behavioral data. Predictions feed visualizations like risk heatmaps, timelines, anomaly graphs, and alert priorities.

After evaluating models based on accuracy (especially on standard cybersecurity datasets like CIC-IDS2017, NSL-KDD, UNSW-NB15), scalability, interpretability, handling of imbalanced data, efficiency for interactive use, and proven applications in cybersecurity prediction, **XGBoost** is selected as the most appropriate model. It consistently delivers high accuracy (often 99%+), excels in tabular/network data common to threat detection, provides feature importance for explainable visualizations, and balances performance with computational efficiency.

2. Introduction

The Interactive Cyber Threat Visualization Dashboard processes real-time or streaming data to detect and predict cyber threats, enabling proactive alerts and user-interactive insights. Threat prediction is central, requiring a model that forecasts attack likelihood, type, or severity from features like packet sizes, protocols, timestamps, and flow statistics.

Key requirements for the model:

- High predictive accuracy to minimize false negatives (missed threats) and false positives (alert fatigue).
- Efficiency for integration into a dashboard (low latency inference).
- Interpretability to support visualizations (e.g., why a threat score is high).
- Robustness to imbalanced classes (attacks are rare).
- Suitability for tabular/time-series network data.

This report reviews 10+ models drawn from cybersecurity literature and benchmarks.

3. Research on AI/ML Models

The models below are commonly applied in intrusion detection systems (IDS), anomaly detection, and cyber threat prediction. Performance references recent studies (2023–2025) on datasets like CIC-IDS2017, NSL-KDD, and UNSW-NB15.

#	Model	Type	Key Strengths	Key Weaknesses	Typical Accuracy (Cybersecurity Datasets)	Relevance to Dashboard Prediction
1	Decision Tree	Tree-based	Highly interpretable, fast training	Prone to overfitting, unstable	~90–95% (NSL-KDD/CIC-IDS)	Basic classification; limited for complex prediction
2	Random Forest	Ensemble (bagging)	Robust, handles imbalance well, feature importance	Slower inference than single trees, memory-heavy	99.42–99.90% (UNSW-NB15/CIC-IDS2017)	Strong baseline; good for multi-class threat types
3	Support Vector Machine (SVM)	Kernel-based	Effective in high dimensions	Slow on large data, sensitive to tuning	~93–98%	Precise separation; scales poorly for real-time
4	Naive Bayes	Probabilistic	Very fast, good for text-like features	Assumes independence (often violated)	~85–95%	Quick filtering; weak on correlated network features

5	Logistic Regression	Linear	Simple, interpretable, probabilistic outputs	Assumes linearity, struggles with complex patterns	~90–97%	Baseline risk scoring for visualizations
6	XGBoost	Gradient boosting	State-of-the-art accuracy, handles imbalance/missing values, fast with optimization, built-in feature importance	Requires tuning, can overfit without regularization	99.20–99.97% (CIC-IDS2017/UNSW-NB15/NSL-KDD)	Excellent for prediction; supports real-time & explainability
7	Artificial Neural Network (ANN)	Deep feedforward	Captures non-linear patterns	Black-box, high compute, needs large data	~95–99%	Complex patterns; less interpretable for dashboard
8	Long Short-Term Memory (LSTM)	Recurrent DL	Handles sequential/temporal data well	Computationally expensive, training slow	~90–99% (with hybrids)	Temporal threat evolution; high resource use
9	Convolutional Neural Network (CNN)	Deep convolutional	Strong feature extraction from structured data	Resource-intensive, better for image-like inputs	~95–99% (hybrids)	Useful for pattern-based logs; overkill for tabular
10	Hybrid Models (e.g., CNN-LSTM, XGBoost-LSTM)	Combined DL/ML	Leverages strengths of multiple approaches	Complex implementation, high compute	99%+ (e.g., FFNN-XGBoost hybrids)	Advanced prediction; integration complexity

Sources & Notes: Accuracies from recent benchmarks (2024–2025) show ensemble methods like XGBoost and Random Forest often outperform or match deep learning on tabular cybersecurity data, especially CIC-IDS2017 (near-perfect separation) and UNSW-NB15 (complex attacks).

4. Selection of the Most Appropriate Model

Chosen Model: XGBoost

Rationale (based on project-specific criteria):

- **Accuracy & Predictive Performance** — Consistently achieves top-tier results: 99.97% on CIC-IDS2017, 99.20% on UNSW-NB15, 78–99%+ on NSL-KDD/IoT variants (often with SMOTE/PCA for imbalance). Outperforms or matches Random Forest/LSTM hybrids in many studies, with superior handling of rare attacks.
- **Efficiency & Scalability** — Faster inference than deep models (LSTM/CNN); supports GPU acceleration and quantization for edge/real-time use. Suitable for streaming dashboard data.
- **Interpretability** — Built-in feature importance and SHAP integration explain predictions (e.g., "high packet rate + unusual protocol → high threat score"), directly feeding dashboard visuals like importance bars or decision path trees.
- **Handling Cybersecurity Challenges** — Excellent with imbalanced data (via scale_pos_weight), missing values, and categorical features. Proven in IDS, botnet detection, IoT threats, and risk prediction.
- **Comparison to Alternatives** — Beats simpler models (e.g., Logistic Regression) on complex patterns; more efficient/interpretable than deep models (LSTM/ANN) for tabular network data; often edges Random Forest in accuracy/speed.
- **Dashboard Fit** — Probabilistic outputs enable risk scoring/heatmaps; feature importance enhances interactive drill-down; supports real-time prediction for proactive alerts.

Alternatives like Random Forest (very close) or LSTM (for pure sequences) were considered but XGBoost offers the best overall balance.

5. Detailed Analysis of the Chosen Model: XGBoost

5.1 Overview and Primary Uses in Cybersecurity

XGBoost is an optimized distributed gradient boosting library implementing tree ensemble learning. It builds trees sequentially, minimizing a regularized loss function.

Key cybersecurity applications:

- Intrusion/anomaly detection (classifying traffic as benign/malicious).
- Multi-class attack type prediction (e.g., DDoS, phishing, ransomware).
- Threat forecasting (predicting attack probability from historical patterns).
- Risk quantification (e.g., expected loss in FAIR-XGBoost hybrids).
- IoT/ IIoT/botnet detection with imbalance handling (SMOTE integration).

In the dashboard, XGBoost processes features (e.g., flow duration, packet count, protocol) to output threat probabilities/scores, enabling visualizations like predictive timelines or prioritized alert lists.

5.2 Accuracy and Performance Metrics

Recent studies (2023–2025) demonstrate exceptional results:

- **CIC-IDS2017**: 99.97% accuracy, high precision/recall/F1 (~99%).
- **UNSW-NB15**: 99.20–99.42% (binary/multi-class), often with hybrids.
- **NSL-KDD**: 78–99% (varies by setup; strong with optimization).
- **IoT/Other**: 99.68–99.99% (e.g., with PCA/SMOTE on TON-IoT, Bot-IoT).
- **Hybrids/Optimized**: Quantized XGBoost reaches 99.93–99.99%; often tops baselines (Random Forest, DNN, SVM).

These high metrics stem from gradient optimization, regularization (preventing overfitting), and imbalance handling—critical for reliable prediction where missing threats is costly.

5.3 Integration into the Dashboard

- **Prediction Pipeline**: Train on labeled datasets → fine-tune on project data → deploy for inference on streaming inputs.
- **Visualization Support**: Use SHAP/feature importance for explainable charts; output probabilities for dynamic risk gauges.
- **Real-Time Capability**: Low-latency inference suits interactive updates.
- **Future Enhancements**: Hybrid with LSTM for temporal boosts if sequences dominate.

6. Conclusion and Recommendations

XGBoost is the optimal model for the Interactive Cyber Threat Visualization Dashboard. Its superior accuracy (consistently 99%+ on key benchmarks), efficiency, interpretability, and proven cybersecurity track record make it ideal for accurate threat prediction and enhanced user insights.

Recommendations:

- Use SMOTE/PCA for imbalance and dimensionality.
- Integrate SHAP for explainability in visuals.
- Evaluate quantized/lightweight versions for performance.
- Compare with Random Forest in prototyping for confirmation.

This selection positions the dashboard for reliable, actionable cyber threat prediction.