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

Summary

This report evaluates more than 10 AI and machine learning models to identify the best option for predicting cyber threats in an interactive visualization dashboard. The dashboard is designed to detect intrusions, anomalies, and malware using network traffic, system logs, and user behaviour data. Since the system is meant to support real-time or near-real-time monitoring, the model must be both fast and highly accurate. The predictions are presented through visuals such as risk heatmaps, timelines, anomaly graphs, and alert priorities to help security teams quickly understand and react to threats.

Each model is tested using standard cybersecurity datasets like CIC-IDS2017, NSL-KDD, and UNSW-NB15. The evaluation considers several important factors, including prediction accuracy, ability to handle imbalanced data, scalability for large data streams, interpretability of results, and computational efficiency for interactive use. While simpler models are easier to explain and deep learning models can capture complex patterns, both have limitations when used in real-time dashboards due to either lower accuracy or higher resource requirements.

After comparing all the models, XGBoost is selected as the most suitable choice. It consistently achieves very high accuracy, often above 99%, and performs especially well on tabular and network-based data commonly found in cyber threat detection. XGBoost also provides feature importance, which helps explain why a threat was detected and supports meaningful visualizations. Its balance of performance, speed, and explainability makes it an excellent fit for an interactive cyber threat visualization dashboard.

Introduction

The Interactive Cyber Threat Visualization Dashboard is designed to work with real-time or continuously streaming data so that cyber threats can be detected and predicted as they happen. Instead of reacting after an attack occurs, the system helps security teams take proactive action by generating early alerts and showing interactive insights through visual elements like risk scores, timelines, and anomaly graphs. This makes threat prediction the core part of the dashboard.

For effective threat prediction, the system needs a machine learning model that can estimate the likelihood, type, or severity of cyber attacks using different input features. These features include network-level information such as packet sizes, communication protocols, timestamps, flow duration, and other traffic statistics. By learning patterns from this data, the model can identify suspicious behaviour before it turns into a serious security incident.

To meet the needs of an interactive dashboard, the selected model must satisfy several important requirements. High predictive accuracy is crucial to avoid missing real threats (false negatives) and to prevent too many unnecessary alerts (false positives), which can overwhelm security analysts. The model must also be efficient, producing predictions with low latency so the dashboard remains responsive during live monitoring.

Interpretability is another key requirement, as the dashboard should not only show that a threat exists but also explain why the threat score is high. This supports meaningful visualizations and helps analysts trust the system. Since cyber attack data is usually imbalanced, with far fewer attack samples than normal traffic, the model must be robust to class imbalance. Finally, the model should be well-suited for handling tabular and time-series network data, which are common formats in cybersecurity monitoring systems.

Based on these needs, the report reviews and compares more than 10 machine learning models that are commonly used in cybersecurity research and industry benchmarks. Each model is evaluated to determine how well it fits the real-time, visual, and analytical demands of the interactive cyber threat dashboard.

- **High predictive accuracy** to reduce missed attacks (false negatives) and avoid excessive alerts that lead to analyst fatigue.
- **Low-latency performance** to ensure the dashboard remains smooth and responsive during real-time data processing.
- **Strong interpretability** so users can understand why a certain threat score or alert is generated.
- **Ability to handle imbalanced data**, as real attack events are much rarer than normal network traffic.
- **Compatibility with tabular and time-series data**, which are standard formats in network monitoring.
- **Scalability** to handle large volumes of streaming data without performance degradation.
- **Stability over time**, so the model can adapt to evolving attack patterns with periodic updates.

To address these requirements, the report reviews more than 10 machine learning and deep learning models drawn from existing cybersecurity literature and benchmark studies. Each model is analyzed in terms of accuracy, efficiency, interpretability, scalability, and real-world usability. This comparative evaluation helps in selecting the most suitable model for powering an interactive, reliable, and explainable cyber threat visualization dashboard.

Research on AI/ML Models

The models below are **commonly applied in intrusion detection systems (IDS), anomaly detection, and cyber threat prediction** because they have shown strong performance in identifying malicious activity in network and system data. Their effectiveness has been supported by **recent studies (2023–2025)** conducted on widely used cybersecurity datasets such as **CIC-IDS2017, NSL-KDD, and UNSW-NB15**, which are considered benchmarks in threat detection research. These models vary in complexity, interpretability, and computational requirements, offering a range of options depending on the specific needs of a real-time interactive dashboard. When choosing among them, key performance factors include **detection accuracy**, **ability to handle imbalanced data**, **efficiency for fast prediction**, and **explainability**, all of which help ensure reliable and actionable threat prediction in live environments.

S.no	Model	Type	Key Strengths	Key Weakness	Typical Accuracy	Relevance to Dashboard Predection
1.	Decision Tree	Tree-based classifier	• Very easy to understand and interpret • Fast to train and simple to implement	• Prone to overfitting • Small data changes can create very different trees	~90–95% (NSL-KDD, CIC-IDS2017)	Good for basic intrusion classification Limited capability for complex or large-scale threat prediction
2.	Random Forest	Ensemble learning (Bagging)	• Robust and stable compared to decision trees • Handles imbalanced datasets well	• Slower inference than a single tree • Requires more memory	99.42–99.90% (UNSW-NB15, CIC-IDS2017)	Strong baseline model Effective for multi-class attack detection
3.	Support Vector Machine(svm)	Kernel-based classifier	• Performs well in high-dimensional spaces • Effective at separating complex attack boundaries	• Slow on very large datasets • Highly sensitive to kernel and parameter tuning	~93–98%	Precise threat separation Not ideal for real-time dashboards due to scalability issues
4.	Logistic Regression	Linear model	• Simple and highly interpretable • Produces probabilistic outputs useful for risk scoring	• Assumes linear relationships • Struggles with complex attack patterns	~90–97%	Baseline threat scoring Useful for dashboards showing risk probabilities
5.	Naïve Bayes	Probabilistic classifier	• Very fast training and prediction • Works well with text-like or categorical data	• Assumes feature independence, which is often unrealistic in network traffic	~85–95%	Quick anomaly filtering Weak when network features are highly correlated

6.	Artificial Neural Networks(ANN)	Deep feedforward neural network	• Captures non-linear and complex relationships	• Acts like a black box • Requires large datasets and higher computation	~95–99%	Detecting complex threat patterns Limited interpretability for visualization-focused systems
7.	Long Short term memory	Recurrent deep learning model	• Excellent for sequential and time-based data • Learns attack progression over time	• Computationally expensive • Slow training and tuning	~90–99% (often higher in hybrid models)	Modelling temporal attack behaviour Resource-heavy for real-time dashboards
8.	XGBoost	Gradient Boosting (Tree-based ensemble)	• State-of-the-art accuracy • Handles missing values and imbalanced data well	• Requires careful tuning • Can overfit without proper regularization	99.20–99.97% (CIC-IDS2017, UNSW-NB15, NSL-KDD)	Excellent choice for real-time threat prediction Ideal for interactive dashboards combining accuracy and explainabiliy
9.	Hybrid Models (e.g., CNN-LSTM, XGBoost-LSTM)	Combined ML and DL approaches	• Combines strengths of multiple models • Achieves very high predictive performance	• Complex implementation • High computational and deployment cost	99%+ (e.g., FFNN–XGBoost hybrids)	Advanced threat prediction Best for research or high-resource systems
10.	Convolutional Neural Network (CNN)	Deep convolutional model	• Strong at automatic feature extraction • Effective when data is structured like images or matrices	• High computational cost • Often unnecessary for tabular network data	~95–99% (mostly in hybrid setups)	Pattern-based log or traffic analysis Overkill for standard tabular IDS datasets

Selection of the Most Appropriate Model for Cyber Threat Prediction

This project evaluated **10 widely used AI/ML models** for cyber threat prediction in an interactive visualization dashboard. The models were chosen based on their popularity in **intrusion detection systems (IDS)**, **anomaly detection**, and **cybersecurity prediction research**, especially on benchmark datasets such as **CIC-IDS2017, NSL-KDD, and UNSW-NB15**.

Chosen Model: XGBoost

After comparing all 10 models, **XGBoost** was selected as the most suitable model for this project.

Rationale for Choosing XGBoost (Based on Project Criteria)

● Accuracy & Predictive Performance

XGBoost consistently delivers **top-tier accuracy** across standard cybersecurity datasets. Reported results include **99.97% accuracy on CIC-IDS2017**, **99.20% on UNSW-NB15**, and **78–99%+ on NSL-KDD and IoT-based variants**, especially when techniques like **SMOTE** or **PCA** are applied to handle imbalance. In many studies, XGBoost **matches or outperforms Random Forest and even hybrid deep learning models**, particularly in detecting **rare and sophisticated attacks**, which are critical in real-world cybersecurity.

● Efficiency & Scalability

Compared to deep learning models such as **LSTM or CNN**, XGBoost offers **much faster inference**, making it well-suited for **real-time or near-real-time dashboards**. It supports **parallel processing, GPU acceleration, and model quantization**, allowing it to scale efficiently for high-volume streaming data. This makes XGBoost practical for both centralized systems and edge-based deployments.

● Interpretability & Explainability

Interpretability is crucial for an interactive dashboard. XGBoost provides **built-in feature importance scores** and integrates seamlessly with **SHAP explanations**. This allows the system to clearly explain *why* a threat score is high.

● Handling Cybersecurity-Specific Challenges

Cybersecurity data is typically **highly imbalanced**, noisy, and incomplete. XGBoost handles these challenges effectively using parameters such as **scale_pos_weight** for imbalance and native support for **missing values**. It also works well with **categorical and tabular features**, making it reliable across use cases like **intrusion detection, botnet identification, IoT threat analysis, and risk prediction**.

Overview and Primary Uses in Cybersecurity (Short Version)

XGBoost is a fast and optimized gradient boosting algorithm that builds decision trees sequentially to improve prediction accuracy while controlling overfitting. It is widely used in cybersecurity because it works very well with tabular network data and imbalanced attack datasets.

In cybersecurity, XGBoost is used for intrusion and anomaly detection, multi-class attack classification (such as DDoS, phishing, and malware), threat forecasting based on historical patterns, and risk quantification. It is also effective for IoT and botnet detection, especially when combined with imbalance-handling techniques like SMOTE.

In the interactive dashboard, XGBoost analyzes features such as packet count, flow duration, and protocol type to generate threat probabilities or risk scores. These outputs drive visualizations like predictive timelines, heatmaps, and prioritized alert lists, enabling quick and informed security decisions.

Conclusion

- XGBoost is the most suitable model for the Interactive Cyber Threat Visualization Dashboard.
- It consistently achieves **99%+ accuracy** on major cybersecurity benchmarks.
- Offers an excellent balance of **accuracy, speed, and interpretability**.
- Well-proven in real-world cybersecurity applications for threat prediction.

Recommendations

- Use SMOTE / PCA to handle class imbalance and reduce feature dimensions.
- Integrate SHAP to explain predictions clearly in dashboard visuals.
- Evaluate quantized or lightweight versions of XGBoost for faster performance.
- Compare results with Random Forest during prototyping for validation.

Final Note

This model selection ensures **reliable, actionable, and real-time cyber threat insights** for the dashboard.