AI-Based Cybersecurity Threat Prediction: Model Research Report

Abstract

Cybersecurity is facing unprecedented challenges due to evolving attack techniques and the increasing complexity of global digital assets. Artificial intelligence (AI) has radically improved predictive analytics for threat identification. This paper explores the latest AI-based models for cybersecurity threat prediction, evaluates their comparative strengths, and recommends ensemble approaches that maximize detection robustness against both known and unknown threats.[1][2]

Introduction

Traditional rule-based mechanisms and static defenses often fail to capture novel or sophisticated cyber-attacks. The integration of machine learning (ML) and deep learning (DL) into cybersecurity enables proactive detection, rapid anomaly identification, and automated response, marking a paradigm shift in the defense landscape.[3][4]

Related Work

Recent works demonstrate that:

- Predictive analytics powered by AI improves detection accuracy, reducing false positives and boosting response time.[2][1]
- Traditional models (e.g., Logistic Regression, KNN) are easy to interpret but struggle with complex patterns.
- Advanced models (e.g., Random Forests, DNNs, LSTM, Autoencoders) address high-dimensional sequential data and unknown threats.
- Hybrid and ensemble methods consistently outperform single-algorithm approaches, offering broader coverage and resilience.[5][6]

Dataset and Preprocessing

Commonly used datasets:

- CIC-IDS, UNSW-NB15, Edge-IIoTset, and large-scale traffic and intrusion detection logs.[7][8]

Preprocessing steps:

- Data cleaning, duplicate removal, and principal component analysis (PCA) for feature reduction.
- Handling class imbalance and normalization to prepare for robust model training.[8]

Model Architectures Evaluated

Model Type	Dataset	Accuracy (%)	F1-Score	Notable Strengths	Limitations
CNN, Multi-Scale	CIC-IDS	~90	High-90s	Spatial feature learning	Needs RNN for context
LSTM, BiGRU	Edge-IIoTset	~90	~0.90	Sequences, time modeling	More training time
Transformers	CIC-IDS	High	High	Long-range attention	Compute-intensive
Ensemble (RF, LSTM, AE)	CIC-IDS, UNSW	up to 99	up to 0.99	Real-time prediction, anomaly detection	Setup complexity
Isolation Forest, GANs	CIC-IDS	Up to 95	Evaluated by AUC	Anomaly and adversarial robustness	Threshold tuning

Methodology

- Multiple ML and DL models were benchmarked on selected datasets.
- Evaluation used key metrics: accuracy, precision, recall, F1-score, and ROC-AUC.
- Ensemble and hybrid models (Random Forest + LSTM + Autoencoder) showed superior results by combining characteristics, providing real-time adaptation and zero-day coverage.[7][8][5]

Results and Discussion

- Ensemble models surpassed individual algorithms, delivering higher accuracy, precision (up to 98.64%), and resilience to new attack types.
- AI-driven systems adapt rapidly, lowering response times and improving detection—even for previously unseen attacks.[8][2]
- Efforts to improve explainability (using SHAP, LIME, Grad-CAM) are essential for stakeholder trust in AI decisions.[6]

Conclusion and Recommendations

A hybrid ensemble of Random Forest, LSTM, and Autoencoder is recommended for cyber threat prediction, balancing speed, interpretability, and anomaly detection. Future developments should focus on continuous learning systems and automated, agentic responses to evolving threats. Practical implementation in cyber defense will require robust tuning, explainable AI, and real-time monitoring capabilities.