# AI & Machine Learning Models Used in Cybersecurity

Artificial Intelligence (AI) and Machine Learning (ML) are transforming cybersecurity by enabling automated detection, analysis, and response to cyber threats. Traditional rule-based systems struggle to detect evolving and zero-day attacks. ML models analyze patterns in large datasets and detect anomalies in real time.

## 1. Random Forest

Used in intrusion detection and malware classification. It combines multiple decision trees to improve accuracy and reduce overfitting. Effective for structured network security data.

## 2. Support Vector Machine (SVM)

Effective for high-dimensional datasets like network traffic logs. Used in spam filtering, malware detection, and intrusion detection systems.

## 3. K-Nearest Neighbors (KNN)

Used for anomaly detection and user behavior analysis. Classifies data based on similarity to nearest neighbors using distance metrics.

## 4. Naive Bayes

Commonly used for email spam detection and phishing identification. Works efficiently with large text-based datasets.

## 5. Artificial Neural Networks (ANN)

Capable of learning complex non-linear attack patterns. Used in malware and botnet detection systems.

## 6. Convolutional Neural Networks (CNN)

Used in malware classification by converting binary files into image-like representations. Excellent for pattern recognition.

## 7. Recurrent Neural Networks (RNN) & LSTM

Best suited for sequential data such as system logs and network traffic over time. Detects brute-force attacks and advanced persistent threats.

## 8. Autoencoders

Powerful for anomaly detection. Learns normal behavior patterns and flags deviations that may indicate cyber threats.

## 9. Gradient Boosting (XGBoost, LightGBM)

Provides high accuracy in fraud detection and malware classification. Handles imbalanced cybersecurity datasets effectively.

## 10. Deep Reinforcement Learning

Used in adaptive cybersecurity systems for automated threat response and dynamic firewall optimization. Learns optimal defense strategies through interaction.

## Conclusion: AI and ML models significantly enhance cybersecurity systems by enabling proactive threat detection, behavior analysis, and automated response mechanisms. Modern cybersecurity solutions often use hybrid approaches combining multiple ML models for improved accuracy and resilience.

Conclusion: AI and ML models significantly enhance cybersecurity systems by enabling proactive threat detection, behavior analysis, and automated response mechanisms. Modern cybersecurity solutions often use hybrid approaches combining multiple ML models for improved accuracy and resilience.