Int Journal of Engineering and Computer Science

Open access

Comprehensive Review Article

Artificial Intelligence-Driven Cybersecurity: Machine Learning Approaches for Threat Detection-A Comprehensive Review

David Kumar[1],*, Sarah Allex[1]

**Department of Biomedical Engineering, National Center for Health Innovation, London, UK*

***Correspondence:** David Kumar, Department of Biomedical Engineering, National Center for Health Innovation, London, UK , E-mail: dvidkumar@gmail,com; DOI: 10.1042/JCTCS.3.1.0005

Abstract

The rapid digital transformation of organizations has significantly increased the complexity and frequency of cyber threats. Traditional cybersecurity mechanisms, which primarily rely on signature-based detection and predefined rules, often struggle to identify sophisticated attacks such as zero-day exploits, advanced persistent threats (APTs), ransomware, and polymorphic malware. Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), has emerged as a promising solution for strengthening cybersecurity by enabling intelligent, adaptive, and real-time threat detection. AI-driven cybersecurity systems analyze large volumes of network traffic, user behavior, and system logs to identify malicious activities with greater accuracy than conventional approaches.

This review presents a comprehensive analysis of AI applications in cybersecurity, focusing on machine learning techniques for intrusion detection, malware analysis, phishing detection, anomaly detection, threat intelligence, and incident response. The article compares supervised, unsupervised, reinforcement, and deep learning approaches while discussing publicly available cybersecurity datasets, evaluation metrics, and deployment challenges. Furthermore, it examines limitations such as adversarial attacks, model explainability, privacy concerns, computational complexity, and regulatory compliance. Finally, the review highlights future research directions including Explainable AI (XAI), federated learning, autonomous security operations, and AI-assisted Security Operations Centers (SOCs).

Keywords: Artificial intelligence, Cybersecurity, Machine learning, Deep learning, Intrusion detection system, Malware detection, Network security, Threat intelligence, Phishing detection, Explainable AI

Received date: Jan 02, 2025; **Accepted date:** Jan 12, 2025; **Published date:** Jan 31, 2025

Citation: David Kumar (2025) Artificial Intelligence-Driven Cybersecurity: Machine Learning Approaches for Threat Detection-A Comprehensive Review. Int J Eng Comp Sci. 3: 1.

Introduction

Cybersecurity has become one of the most critical challenges of the digital era. Governments, businesses, healthcare providers, financial institutions, and educational organizations increasingly depend on interconnected digital infrastructures that process sensitive information and support mission-critical services. While digital transformation has improved efficiency and innovation, it has also expanded the attack surface available to cybercriminals.

Traditional security mechanisms-including firewalls, antivirus software, and signature-based intrusion detection systems—remain important but have limitations when confronted with rapidly evolving cyber threats. Modern attackers employ techniques such as encrypted malware, fileless attacks, social engineering, ransomware, botnets, and advanced persistent threats that can evade static detection methods. Consequently, cybersecurity strategies are shifting toward intelligent, adaptive approaches capable of learning from data and identifying previously unseen attack patterns.

Artificial Intelligence (AI) has become a key enabler of this transition. Machine learning algorithms can analyze large volumes of network traffic, system logs, and user behavior to distinguish normal activity from malicious behavior. Unlike conventional rule-based systems, AI models continuously improve as they are trained on new data, enabling faster detection of emerging threats.

Applications of AI in cybersecurity span multiple domains, including:

- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- Malware classification
- Phishing and spam detection
- Network anomaly detection
- User and Entity Behavior Analytics (UEBA)
- Threat intelligence
- Vulnerability assessment
- Security Operations Center (SOC) automation
- Incident response and digital forensics

Among these applications, intrusion detection has attracted particular attention due to its ability to identify unauthorized activities before significant damage occurs. Deep learning architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Graph Neural Networks (GNNs), and Transformer-based models have demonstrated promising performance in detecting complex attack patterns that traditional systems may miss.

Despite these advances, AI-driven cybersecurity faces several challenges. Machine learning models require high-quality training data and may be vulnerable to adversarial attacks designed to manipulate predictions. Additional concerns include false positives, interpretability, privacy protection, computational requirements, and integration with existing enterprise security infrastructures.

This review aims to synthesize current research on AI-driven cybersecurity by examining machine learning techniques, practical applications, benefits, limitations, and future research opportunities. It is intended to provide researchers and practitioners with a consolidated overview of how AI is reshaping modern cybersecurity practices.

Objectives of the review

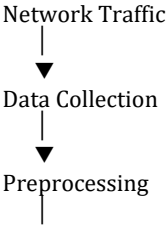
The objectives of this review are to:

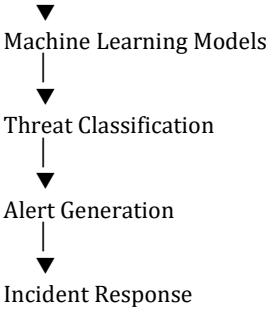
- Examine the role of Artificial Intelligence in modern cybersecurity.
- Compare machine learning techniques used for cyber threat detection.
- Review AI applications in malware detection, phishing prevention, intrusion detection, and threat intelligence.
- Discuss current challenges and limitations.
- Identify future research directions for intelligent cybersecurity systems.

Table 1. Major applications of AI in cybersecurity.

Application area	AI techniques	Primary objective
Intrusion Detection	Machine Learning, Deep Learning	Detect unauthorized access
Malware Detection	CNN, Random Forest, Gradient Boosting	Identify malicious software
Phishing Detection	NLP, Transformers	Detect fraudulent emails and websites
Network Traffic Analysis	LSTM, Autoencoders	Identify anomalous traffic
Threat Intelligence	NLP, Knowledge Graphs	Analyze cyber threat reports
User Behavior Analytics	Clustering, Anomaly Detection	Detect insider threats
Incident Response	Reinforcement Learning	Automate security response

Figure 1: AI-Driven cybersecurity framework.




Machine Learning Models
Threat Classification
Alert Generation
Incident Response