AI-Based Cybersecurity Threat Detection System

Amit Kumar bachcha jha
Sonopant Dandekar Shikshan Mandali College

Abstract- In the evolving landscape of digital transformation, cyber threats have become increasingly sophisticated. Traditional security systems often struggle to identify complex and dynamic attack patterns. This paper explores an AI-based cybersecurity threat detection system that leverages machine learning algorithms to detect anomalies and potential threats in real-time. By utilizing data-driven techniques such as supervised and unsupervised learning, AI enhances detection accuracy and response speed. This research outlines the architecture, implementation strategies, benefits, and limitations of AI-based security systems in modern enterprises.

Keywords-Artificial Intelligence, Cybersecurity, Machine Learning, Threat Detection, Intrusion Detection Systems

1. INTRODUCTION

Cybersecurity is a fundamental component of information technology infrastructure. With the rapid expansion of connected systems and digital services, cyber threats such as phishing, malware, and ransomware have become more prevalent. Traditional Intrusion Detection Systems (IDS) rely on static rules and known signatures, which limit their effectiveness against novel or evolving threats. The integration of Artificial Intelligence (AI), particularly Machine Learning (ML), presents a new paradigm in proactively identifying and mitigating cyber threats.

2. AI IN CYBERSECURITY

AI, especially ML, enables systems to learn from historical data and recognize patterns indicative of malicious activity. Key ML techniques applied in threat detection include:
- Supervised Learning: Uses labeled datasets to train models that classify behaviors as benign or malicious.
- Unsupervised Learning: Identifies anomalies in unlabeled data that may represent previously unknown threats.
- Reinforcement Learning: Continuously adapts detection strategies based on feedback from system performance.

These approaches allow the system to detect threats in real-time, reducing the reliance on human analysts and manual threat identification.

3. SYSTEM ARCHITECTURE

An AI-based cybersecurity system typically consists of the following components:
- Data Collection: Logs and network traffic data are collected from endpoints and servers.
- Preprocessing: Data is cleaned, normalized, and structured for analysis.
- Feature Engineering: Key attributes are extracted to train and test ML models.
- Model Training and Deployment: ML models are trained to detect anomalies and are integrated into the monitoring infrastructure.
- Alerting and Response: Detected threats trigger alerts and, in some cases, automated mitigation procedures.

4. BENEFITS

- Real-Time Detection: Enables proactive threat management.
- Scalability: Can handle vast amounts of data across multiple endpoints.
- Reduced False Positives: ML models improve accuracy over time, reducing unnecessary alerts.

5. CHALLENGES AND LIMITATIONS

- Data Quality: Requires large, high-quality datasets for training.
- Adversarial Attacks: AI models can be targeted by attackers using evasion techniques.
- Interpretability: Black-box nature of some models makes it hard to understand decision-making.

6. CONCLUSION

AI-based cybersecurity systems represent a significant advancement over traditional security methods. By leveraging machine learning, organizations can detect and respond to threats more effectively. However, continuous improvement, transparency, and integration with human oversight are essential for building trust and reliability in these systems.