

Tentative Title

AI-Driven Threat Detection and Response Systems for Next-Generation Cybersecurity.

Introduction

Modern organizations face increasingly sophisticated cyber threats that require advanced defensive strategies. The integration of artificial intelligence (AI) into cybersecurity provides opportunities to enhance detection, automate incident response, and build resilient security systems capable of adapting to emerging risks.

Research Problem

Traditional cybersecurity solutions struggle with the speed, complexity, and adaptability of modern threats. Attackers can rapidly modify tactics, evading signature-based detection and overwhelming manual response teams. This proposal aims to address the gap by developing AI-powered frameworks capable of identifying and responding to threats in real time.

Objectives

- Develop machine learning models for automated threat detection and classification in network traffic and system logs.
- Design AI-driven incident response protocols that minimize manual intervention and speed up recovery.
- Evaluate effectiveness of AI-based security solutions against adversarial attacks and evolving threat landscapes.
- Investigate ethical and privacy implications of deploying AI in cybersecurity systems.

Methodology

- Conduct literature review on current AI and machine learning techniques used in cybersecurity.
- Collect and preprocess cyber threat datasets; train supervised and unsupervised models for anomaly detection and predictive analytics.
- Simulate cyberattacks in controlled environments to test model performance and robustness.
- Collaborate with industry partners to validate the solution in real-world scenarios.
- Analyze data for false positives, adaptability, scalability, and ethical concerns.

Expected Outcomes

- Novel AI models capable of detecting previously unseen attack vectors.
- Automated response protocols reducing average incident resolution time.
- Publications on best practices and practical frameworks for AI integration in cybersecurity.
- Recommendations for responsible use of AI in data protection and privacy.