Artificial Intelligence for Cybersecurity: A Review

Tung (Francis) Cu
College of Business and Management
Northeastern Illinois University
Email: tcu@neiu.edu

Abstract

The next generation of Artificial Intelligence (AI) and Machine Learning (ML) are increasingly incorporated in cybersecurity solutions. Experts predict that, over time, companies will incorporate AI into every cybersecurity product portfolio. While AI and ML increase the defenders' capability to detect and prevent abnormal behavior patterns, attackers are also using AI and ML to learn about a target's vulnerabilities and launch attacks.

The purpose of this study is to conduct a literature review on a series of original research papers, both theoretical and empirical, to identify current challenges and issues of AI aid, misuse and threat in cybersecurity in different contexts such as business, healthcare, education, politics, and economics. To this end, the paper classifies previous AI studies into four different categories: Artificial Neural Network applications, Intelligent Agent applications, Artificial Immune System applications, Genetic Algorithm and Fuzzy Sets applications. The paper conducts a review of these applications on three main criteria: system response, system robustness and system resilience.

The assessment shows that, regarding the system response, AI will improve the response capabilities and countering measures of cyber-defense systems. At the same time, it will expand the targeting ability of attackers, enabling them to use more complex and richer attacks. As more separate AI systems are connected to, the risk of serious consequences from malevolent interference may increase. Regarding the system robustness, AI can improve software design to a new level that is capable of self-testing and self-healing. However, as AI systems to make deductions and decisions without human involvements, they could be compromised and go undetected for a long time. Besides, delegating software design and testing to AI could lead to a complete deskilling of experts who need to keep testing systems so that they still can detect abnormal if AI can't or gets it wrong.

To be resilient, security systems need a huge data volume from scanning of every mouse click, monitor files, emails, mobile and endpoint devices, or even traffic data on a network to train their pattern recognition. This implies that AI can improve system resilience to attacks, but this requires extensive monitoring of the system and comprehensive data collection. This makes the system itself prone to attack even more. The paper concludes with recommendations to improve the response, robustness and resilience capability of AI systems.

Keywords: Artificial Intelligent, Cyber Security, Artificial Neural Network, Machine Learning