Chapter 8
Artificial Intelligence–Powered Cybersecurity: The Future of How Threats Are Detected and Responded

Soumya George
https://orcid.org/0000-0002-7256-7677
SGC Aruvithura, India

ABSTRACT

Cybersecurity threats are ever-changing and characterized by more sophisticated attacks including, but not limited to, ransomware, phishing attempts, and Distributed Denial-of-Service (DDoS) attacks. Integration of Artificial Intelligence in cybersecurity is one of the pioneering methods for dealing with the new threats in the digital environment. This article highlights areas where AI technologies improve threat detection, response automation, and risk management. It discusses the challenges, ethical issues, and AI solutions in cybersecurity

INTRODUCTION

Cybersecurity threats are basically harmful actions that target the confidentiality, integrity, or availability of digital systems and data. Some of the most common threats include malware (like viruses, ransomware, spyware, and Trojans), phishing (which involves sending deceptive emails or messages to trick people into giving up sensitive information), Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks (where systems are overloaded to disrupt access), and Man-in-the-Middle (MitM) attacks (that involve intercepting communications). There are also insider threats (which come from malicious or careless employees), Advanced Per-

DOI: 10.4018/979-8-3373-1102-9.ch008

sistent Threats (APTs) (that are sustained, targeted attacks by sophisticated groups), and zero-day exploits (which attack unknown vulnerabilities). Other risks include credential theft through techniques like keylogging and brute-force attacks, social engineering tactics (which manipulate individuals into divulging information), supply chain attacks (that compromise third-party vendors), crypto jacking (unauthorized cryptocurrency mining), and vulnerabilities in the Internet of Things (IoT). These challenges are difficult for traditional defenses to deal with. Artificial intelligence (AI) has become an essential support, utilizing complex algorithms to analyze large dataset and detect anomalies and improve decisions (Makridakis, 2017)

This paper discusses various cybersecurity threats, AI methodologies in cybersecurity, explores its real-world applications, and examines its advantages and limitations, concluding with recommendations for future research.

Glossary of Cybersecurity Threats

The various types of cybersecurity threats are listed below:

1. **Adware**: Automatically displays advertisements, downloads advertisements when installed on a computer, mostly accompanying free software which may lead the device to slugging down, diffusing it to unwanted websites (Symantec, 2024).
2. **Advanced Persistent Threats (APT)**: There are very long, targeted cyber-attacks, when they reach in to penetrate the networks and stay there, undetected, stealing sensitive information (FireEye, n.d.).
3. **Botnets**: These are networks of compromised devices controlled by attackers to use them to execute different needs like sending out spam, stealing data, and performing DDoS attacks among other functions.
4. **Brute Force Attack**: Any dictionary attempt is made to crack passwords and break any type of encryption by trying every possible combination.
5. **Crypto jacking**: The unauthorized use of someone's computing resources to process cryptocurrency mining. It slows devices down and is energy-intensive.
6. **Cross-site Scripting (XSS):** It's where malicious scripts get injected into trusted sites, exploiting vulnerabilities in web applications to compromise user data.
7. **Denial-of-Service Attack (DoS)**: An attack by which a server, network, or service can be made unavailable to the clients through a plethora of unsolicited traffic (Cloudflare, 2024).
8. **Data Breaches:** Unauthorized access to confidential or sensitive data, which are sometimes considered identity thefts or financial losses.
9. **Eavesdropping Attacks**: Interception and stealing data over a network including passwords or credit card information.