Chapter 6
AI-Based Cybersecurity Threat Detection and Prevention

Tina Sharma
Chandigarh University, India

Pankaj Sharma
TrueBlue Headquarters, USA

ABSTRACT

The chapter presents an overview of AI-based cybersecurity threat detection and prevention. It highlights the importance of AI in tackling the ever-increasing threat landscape and explores various techniques and algorithms used in cybersecurity. AI's ability to process real-time data, identify patterns, and provide accurate threat intelligence is emphasized. The chapter covers machine learning, deep learning, and natural language processing, providing practical examples of their application in cybersecurity. Challenges such as data quality and bias are discussed, along with potential solutions. AI-based cybersecurity solutions like intrusion detection systems and threat intelligence platforms are presented. The chapter concludes with a discussion on the future of AI-based cybersecurity, including emerging technologies like quantum computing and blockchain, and the need for ongoing research and development to address evolving threats. Overall, it offers a comprehensive overview of AI's role in cybersecurity, highlighting benefits, challenges, and future directions.

DOI: 10.4018/978-1-6684-9814-9.ch006

INTRODUCTION TO AI-BASED CYBERSECURITY

Cybersecurity refers to the practice of protecting computer systems, networks, and digital assets from unauthorized access, theft, or damage. Cyber threats can come in many forms, including viruses, malware, phishing attacks, and hacking attempts. Effective cybersecurity strategies involve a combination of technology, policies, and user education to prevent, detect, and respond to these threats. For example, a company may use firewalls, intrusion detection systems, and other security technologies to protect its network from external threats. It may also implement policies such as strong passwords and two-factor authentication to prevent unauthorized access to sensitive data. Finally, employee training and awareness programs can help educate users about the risks of cyber threats and how to avoid them.

The importance of cybersecurity has increased in recent years as more organizations rely on digital systems to store and process sensitive information. The cost of a cyber-attack can be significant, including financial losses, damage to reputation, and legal consequences.

Artificial Intelligence (AI) has transformed the field of cybersecurity, enabling organizations to detect and respond to cyber threats with greater speed and accuracy. AI-based cybersecurity systems leverage machine learning algorithms, natural language processing, and other advanced technologies to analyze vast amounts of data and identify patterns that indicate a cyber-attack. By automating many aspects of threat detection and response, AI-based cybersecurity solutions can help organizations improve their overall security posture and reduce the risk of cyber breaches.

According to a report by Gartner, “AI augmentation will create $2.9 trillion of business value and recover 6.2 billion hours of worker productivity by 2021” (Osterman, 2019). This highlights the potential of AI to revolutionize cybersecurity, as it can help organizations detect and respond to cyber threats more efficiently and effectively. AI-based cybersecurity solutions can also help address the growing skills gap in the cybersecurity industry, as they can perform many tasks that would otherwise require highly trained and experienced cybersecurity professionals.

However, the use of AI in cybersecurity also poses new challenges and risks. For example, AI-based systems may be vulnerable to adversarial attacks, where an attacker attempts to manipulate the AI algorithms to evade detection. Additionally, there are concerns about the transparency and explainability of AI-based cybersecurity systems, as it may be difficult to understand how the systems make decisions or identify false positives.

Despite these challenges, the use of AI in cybersecurity is expected to continue to grow in the coming years. Organizations that are able to effectively leverage AI-based cybersecurity solutions will be better equipped to defend against cyber threats and protect their valuable data and assets.