Chapter 9
Artificial Intelligence Applications in Cybersecurity

Tesfahiwet Abrham
Zayed University, UAE

Sanaa Kaddoura
https://orcid.org/0000-0002-4384-4364
Zayed University, UAE

Hamda Al Breiki
Zayed University, UAE

ABSTRACT

For the past decades, cyber threats have been increasing significantly and are designed in a sophisticated way that is tough to detect using traditional protection tools. As a result, privacy and sensitive personal information such as credit card numbers are being continuously compromised. Therefore, it is time to find a solution that can stand against the spreading of such threats. Artificial intelligence, machine learning, and deep learning could be among the top methods of detecting cyber threats. These methods could help to improve the detection technologies and engines for computer network defense. This chapter mainly focuses on artificial intelligence in cybersecurity. The main goal of this chapter is to highlight the drawbacks of the traditional security protection tools and discuss the improvements that has been made so far by applying artificial intelligence to solve the current cybersecurity problems.

INTRODUCTION

Almost every week, an individual's or a company's data is compromised in today's world. Each incident serves as a reminder of the flaws in standard cybersecurity methods. Traditional network protection tools are currently used to protect enterprises from ransomware and complex malware. Those tools, however, are not guaranteed enough for the task as new sophisticated and interconnected cyberattacks are developed (Calderon, 2019). These attacks can adversely affect the information assets of the organization. The most sophisticated tools, including Intrusion Detection and Prevention Systems (IDPS),

DOI: 10.4018/978-1-6684-6937-8.ch009

have been evaded by skilled cybercriminals, making botnets almost impossible to detect. Cyber incidents are hazardous because of central network warfare (Gupta & Sheng, 2019). Reduced sales, operational disruption, additional hiring, and a loss of competitive edge are just a few examples of the harm that can result from theft or penalties. Threats are becoming viral worldwide, so computer network defense technologies cannot quickly adapt to next-generation cybersecurity threats due to their discovery and detection engine limitations.

To reduce the destructive effects of cyber threats, we need to find a solution designed to provide complete protection against a wide range of attacks. Security teams need to always think like a hacker to understand the techniques and goals of the actual attack. Currently, experts are using Artificial Intelligence (AI) to get ahead of cyber criminals so that they can counter new attacks (Jean-Philippe, 2018). Therefore, to have continuous protection against such attacks, the security systems need a steady adjacent to new threats.

According to Gupta and Sheng, researchers, governments, and public and private companies or organizations are all working hard to reach an ideal level of cybersecurity protection in which they can safeguard their information assets or systems with the most efficient and cutting-edge technologies (Gupta & Sheng, 2019). Consequently, artificial intelligence and machine learning have become crucial tools for cybersecurity systems to collaborate with humans in the face of cyber threats and other obstacles. AI and machine learning (ML) landscape prioritize threat detection, and businesses rely on AI and ML for faster responses, better outcomes, and increased productivity.

Many researchers suggest that AI and ML may be the future paradigms in cybersecurity automation. Using predictive analytics to form statistical inferences, AI and ML can help reduce cyber dangers while using fewer resources (LAZIĆ, 2019). In the subject of cybersecurity, AI and ML can help detect new attacks more quickly and provide an effective tool for drawing statistical inferences and pushing that information to endpoint security systems. Due to a significant number of attacks and a shortage of cybersecurity workers, AI and ML are becoming increasingly vital tools.

AI and ML are valuable and powerful tools in today's technology. AI and ML have demonstrated their worth by deciphering data from various sources and spotting crucial relationships that people would miss. On the other hand, hackers are skilled enough- they can develop tools to stand against AI and may use it for offensive reasons. Therefore, businesses and governments should consider incorporating AI into their systems. The rapid advancements and growth of AI technology, causes cybersecurity norms and standards to continuously expand and change not be tracked by the new tools. With the versatility of AI applications, hackers will use AI approaches to avoid detection. As a result, having another AI machine is an excellent way to deal with an AI threat from hackers (McAfee Labs 2019). The three critical issues explored in this chapter are the influence of AI and ML on cybersecurity, the benefits and drawbacks of employing AI tools for security, and whether AI and ML can assist the cybersecurity industry in reducing cyber risks.

CYBERSECURITY

In the present, the internet makes the world a small village in many ways, but it has also exposed us to influences that have never been so diverse and difficult. The realm of hacking expanded as quickly as security. Privacy and information protection are the primary security practices that each organization is concerned with (Rajasekharaiah et al., 2020). Due to the evolving nature of threats online, people are