Chapter 6
Artificial Intelligence and Cybersecurity

Rupam Hazra
https://orcid.org/0009-0003-0332-2128
Global Institute of Management and Technology, India

Parag Chatterjee
https://orcid.org/0000-0003-1243-9582
Global Institute of Management and Technology, India

Yash Singh
Global Institute of Management and Technology, India

Gopal Podder
https://orcid.org/0009-0000-7736-9605
Global Institute of Management and Technology, India

Titli Das
https://orcid.org/0009-0001-3774-1828
Global Institute of Management and Technology, India

ABSTRACT

The integration of Artificial Intelligence (AI) into cybersecurity has become a transformative approach in defending against the increasing sophistication of cyber threats. As traditional security mechanisms struggle to keep pace, AI offers advanced tools such as machine learning, behavioral analytics, and natural language processing to enhance threat detection, incident response, and malware prevention. AI's ability to analyse vast datasets, detect anomalies in real-time, and predict future threats is revolutionizing cybersecurity practices. While AI presents numerous benefits, including automation of time-consuming tasks and proactive defense, ethical and

DOI: 10.4018/979-8-3373-2282-7.ch006

privacy considerations must be addressed to ensure fairness and transparency in its deployment. This chapter explores AI's critical role in modern cybersecurity, its techniques and applications, and the challenges that need to be navigated as AI continues to evolve in the field.

INTRODUCTION

In the era of digital technology, cybersecurity is now a top priority for individuals, organizations, and governments. The swift growth of linked devices, cloud services, and internet platforms has generated a large attack surface for cybercriminals. As cyber threats grow more complex, conventional security measures like firewalls, antivirus programs, and signature-based detection—frequently fail to adapt to changing attack methods. To tackle this challenge, the incorporation of Artificial Intelligence (AI) into cybersecurity has surfaced as a revolutionary answer.

Artificial Intelligence, due to its capability to examine large datasets, identify patterns, and adjust to emerging threats, provides considerable benefits compared to traditional security approaches. AI technologies, such as machine learning (ML), natural language processing (NLP), and Behavioral analytics, enable security systems to identify, thwart, and react to cyberattacks instantly. AI can recognize previously undiscovered threats by analysing data and consistently enhancing its detection skills. Additionally, AI has the capability to automate labour-intensive tasks like surveillance, data evaluation, and incident management, greatly improving the efficiency and scalability of security operations.

Introduction to Artificial Intelligence and Cybersecurity

Artificial Intelligence (AI) has emerged as a transformative technology that is reshaping numerous industries, including cybersecurity. These processes include learning (the ability to improve performance based on experience), reasoning (the ability to draw conclusions), and self-correction. In the context of cybersecurity, AI plays a vital role in identifying, preventing, and responding to security threats, which are becoming increasingly sophisticated and complex. The process of making a computer, computer-controlled robot, or software think intelligently in a way that is comparable to that of intelligent humans is known as artificial intelligence. (Welukar, Jenis N., and Gagan Prashant Bajoria,2021). AI is being utilized in cybersecurity in various ways, such as through machine learning (ML) algorithms that can detect unusual patterns of behaviour within network traffic, enabling the identification of potential cyberattacks. By using large datasets, AI systems can predict vulnerabilities, automate threat detection, and optimize the allocation of resources