# Chapter 22
# Artificial Intelligence in Cyber Security

**MohanaKrishnan M.**
*Hindusthan College of Arts and Sciences, India*

**A.V. Senthil Kumar**
*Hindusthan College of Arts and Sciences, India*

**Veera Talukdar**
*RNB Global University, India*

**Omar S. Saleh**
*School of Computing, Universiti Utara Malaysia, Malaysia*

**Indrarini Dyah Irawati**
*Telkom University, Indonesia*

**Rohaya Latip**
*Universiti Putra Malaysia, Malaysia*

**Gaganpreet Kaur**
*Chitkara University Institute of Engineering and Technology, Chitkara University, India*

## ABSTRACT

*In the digital age, cybersecurity has become an important issue. Data breaches, identity theft, captcha fracturing, and other similar designs abound, affecting millions of individuals and organizations. The challenges are always endless when it comes to inventing appropriate controls and procedures and implementing them as flawlessly as available to combat cyberattacks and crime. The risk of cyberattacks and crime has increased exponentially due to recent advances in artificial intelligence. It applies to almost all areas of the natural and engineering sciences. From healthcare to robotics, AI has revolutionized everything. In this chapter, the authors discuss certain encouraging artificial intelligence technologies. They cover the application of these techniques in cybersecurity. They conclude their discussion by talking about the future scope of artificial intelligence and cybersecurity.*

DOI: 10.4018/978-1-6684-8098-4.ch022

## INTRODUCTION

The rise of digital technology has transformed the way we live, work, and communicate. As our reliance on technology grows, so too does the need for effective cyber security measures. Cyberattacks are becoming increasingly sophisticated and frequent, with criminals and nation-states targeting everything from financial institutions to critical infrastructure. Traditional cyber security measures are no longer sufficient to defend against these threats, and organizations are turning to artificial intelligence (AI) to enhance their capabilities.AI has the potential to revolutionize cyber security by enabling organizations to detect and respond to threats in real-time. Machine learning, deep learning, and natural language processing are just a few of the AI techniques that are being used to identify and respond to cyber threats. However, the implementation of AI in cyber security also presents significant challenges, including issues of bias, and ethical concerns.

Cybersecurity is fundamental because it guards against theft and devastation to all kinds of information. This covers delicate information, personally identifiable information (PII), protected health information (PHI), personal data, data pertaining to intellectual property, and information networks used by the government and business. Your company cannot help shield selves from data breach campaigns without an information security program, trying to make it an unavoidable target for cybercriminals.

Due to increased global connectivity as well as the utilization of cloud services like Amazon Web Services to keep private and sensitive data, both inherent risk and residual risk are developing (Alhayani et al., n.d.). The risk that your corporation will experience an effective cyberattack or data breach is increasing as a consequence of widespread poor configuration of cloud services and increasingly savvy cybercriminals.

Business leaders could perhaps solely depend on conventional cybersecurity instruments like firewalls and antivirus software because cybercriminals are becoming more cunning and their methodologies are becoming more susceptible to conventional cyber countermeasures. To remain protected, it's crucial to cover all aspects of cybersecurity.

Cyber challenges can originate at any level in less your company. To inform staff about common cyberthreats like social engineering scams, phishing, ransomware attacks (think WannaCry), and other malware developed to steal intellectual property or personal data, workplaces must also provide cybersecurity awareness training.

Given the increasing prevalence of information leakage, cybersecurity is important across all sectors, not just those with strict regulations like the healthcare sector. Following a data breach, even smaller businesses run the risk of experiencing irreversible reputational damage.

Programs that are using artificial intelligence are also susceptible to direct assaults. By tampering with the information, it is possible to change the usefulness of Machine Learning (ML) algorithms. The data that is fed to the AI causes it to behave as designed. If false positives are provided, those who depend on the system's intelligence would suffer negative effects. This might also occur as a result of coding flaws like software defects. This issue can be solved with adequate testing tools and bug reward schemes, but measures to help protect the ML algorithms theown are still being developed.