Chapter 6
Application of Artificial Intelligence in Cybersecurity

Geetika Munjal
https://orcid.org/0000-0001-5213-9993
Amity Univesity, Noida, India

Biswarup Paul
Amity Univesity, Noida, India

Manoj Kumar
https://orcid.org/0000-0001-5113-0639
University of Wollongong, UAE

ABSTRACT

Cybersecurity is the knowledge and practice of defending computers, mobile devices, servers, electronic devices, networks, and precious data from malicious attacks. Traditional security methods have advantages in various ways, but they may sometimes seem to be ineffective due to lack of intelligence and vitality to meet the current diverse needs of the network industry thus latest techniques need to be developed to handle these threats. The developments in Artificial intelligent (AI) techniques have simplified life by providing efficient solutions in different domains including cyber security. This chapter has reviewed existing tools of cyber security, highlighting different ways artificial intelligence can be applied in providing Cybersecurity solutions. AI-based security systems make decisions for helping people, it is particularly worrying that these systems do not currently have any moral code thus current chapter also highlights the need to ethical code in providing AI solution for cyber security.

DOI: 10.4018/979-8-3693-1431-9.ch006

1. INTRODUCTION

In the last two decades, information and communication sector has evolved a lot, bringing with it a seamless integration of technology with the day-to-day life. It provides a platform for communication, networking and digitization benefiting the entire world. This rise information technology has shifted the world paradigm with human using it to automate and semi automate various operations like businesses, healthcare, banking, finance, manufacturing, transportation, logistics, customer services, human resource, media, governments activities, defence, and various other fields. Thus, it can be said that cyberspace comprises of various infrastructures and systems built on and comprising of vital and sensitive data which serves the interests of governments, companies and general public. This development in cyberspace has not only brought immense opportunities but also unprecedented challenges. Arguably the biggest challenge in current digital world is keeping this space where different aspects of citizens lives are intertwined as secured and it can be termed as Cybersecurity. Cybersecurity can be explained as a set of technologies and channels used to safeguard computer software, hardware, applications, networks, programs against vulnerabilities via cyber criminals, malicious organizations, and hackers. It also prevents the unauthorized access to data belonging to both public and private sector. It is a complete assortment responsible for defending networks and data, applicable at network, host, data and application level (Buczak & Guven, 2015). A cyber-attack can be described as a malicious attempt to compromise, hinder, harm, gain unauthorized access and manipulate a computer system, network, digital device. Such an attack can be carried out by individuals, groups, or organizations with malicious intentions like stealing money, data or simply compromising vital systems and supply chains.

Artificial Intelligence (AI) is a field in computer science that includes complex mathematical models, analysing the data for correlations and patterns, and using these patterns to make predictions about future states and imitating human behaviour like thinking, planning, generating ideas, understanding speech and visuals . It can be a tool integrated in software that help us in making an attempt to get the essence of intelligence and developing intelligent machines that are able to assist us in complex tasks as well as automate them. AI is scaling up to our cognitive abilities and enhancing various fields like healthcare, technology, transport, education and most importantly cyber security (Saha et al., 2020). Due to their transformative abilities and flexible nature, artificial intelligence is being implemented in Cybersecurity to combat the challenges in the dynamic and ever changing cyberspace.

Today AI has been scaled up to our cognitive abilities and enhancing various fields like business healthcare, technology, transport, education and most importantly cyber security (Saha et al., 2020). Due to their transformative abilities and flexible

A Generic, Multi-Period and Multi-Partner Cost Optimizing Model for Cloud-Based Supply Chain

Goknur Arzu Akyuzand Mohammad Rehan (2016). *International Journal of Cloud Applications and Computing (pp. 55-63).*
www.irma-international.org/article/a-generic-multi-period-and-multi-partner-cost-optimizing-model-for-cloud-based-supply-chain/159852