International Journal of Security and Privacy in Pervasive Computing
Volume 15 • Issue 1

Application of Artificial Intelligence in Cyber security

Varun Kharbanda, SP Jain school of global management, Missing Country

Seetharaman A, SP Jain school of global management, Australia

Maddulety K, SP Jain school of global management, Australia

ABSTRACT

Artificial intelligence (AI) has emerged as the most widely applicable field across varied industries. Being an evolving technology, it may be quite useful in sensitive areas such as cyber security where there is a dire need for implementation of AI technologies, such as expert systems, neural networks, intelligent agents, and artificial immune systems. The primary reason for AI fitment to cyber security area is its ability to detect anomalies proactively and predictively in the network, thereby working towards securing the network before the damage related to loss of data and/or reputation is done. There are different types of AI technologies as mentioned above that could be applied in cyber security in its varied forms. In this paper, the emphasis is on specific AI technologies that can bring unique benefits to the cyber security field with its unique applicability to different scenarios. The outcome of this study shows that AI technologies such as expert systems, neural networks, intelligent agents, and artificial immune systems are transforming the landscape for managing cyber threats.

KEYWORDS

Artificial Immune System, Artificial Intelligence, Cyber Risks, Cyber Security, Cyberattacks, Cyberspace, Expert Systems, Intelligent Agent, Machine Learning, Neural Networks

1. INTRODUCTION

Since this article involves understanding how Artificial Intelligence (AI) is going to be applied and its usage in cyber security functions, it is of paramount importance to understand the meaning of AI. AI endeavours to build and recognise smart objects. Employees or users of AI could apply their skills to any industry they deem fit; thus, AI is a broad area in this sense (Russell & Norvig, 2016). At the core, it conveys when the machine starts imitating human intelligence and starts self-learning, leading to unknown solutions – something machine was never capable of doing before. However, algorithmic modelling has made this possible, and AI has become a universal term and function. Moreover, AI technologies such as expert systems, machine learning, deep learning or neural networks, artificial immune system, intelligent agents et cetera are being applied in various fields including but not limited to healthcare, automotive, banking and insurance sectors.

A major problem in corporations these days is how they can guard themselves against possible anomalies. The variety and possibility of these unidentified outbreaks generate the requirements for corporates to prioritise the method in which they protect themselves against such cyberattacks. Thus, each corporate or company is required to understand the attacks that they are most defenceless against

DOI: 10.4018/ijsppc.318676

*Corresponding Author

to reduce the risk of an attack (Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016). With the recent increase in cyberattacks, the uncertainty across the enterprise has increased by leaps and bounds.

Cyberattacks on global company networks, including governments, have kept the cyber-attack prevention teams extremely busy and hence, automation alone will not suffice. However, there is an ever-growing need to handle such cyberattacks proactively and with the ability to predict and resolve them considering the evolution of AI capabilities or techniques, such as neural networks or deep learning, machine learning, expert systems, artificial immune systems, intelligent agents. Such advanced technologies are changing the way cyber security is being managed in modern organisations which are more vulnerable to unknown or unpredictable attacks than ever before. The change is perceived as not just managing these cyberattacks proactively but predicting these attacks and resolving issues before they negatively impact a company's operations and risk customer's data.

This article will explore how the cyber security landscape may be transformed after application of emerging and disruptive technologies like AI in handling cyber risks. Most AI tools are used to enhance cyber security, and cyber risk management tools benefit the whole cyber security process, making them more robust to handle security vulnerabilities in organisational networks. Various types of cyber risks, such as ransomware, phishing, data leakage, hacking, trojan horse, computer worm, DOS and DDOS attack, adware and spyware, were usually managed reactively as per traditional practices which involved incident detection and responding accordingly to safeguard company's network. However, with increasingly sophisticated network attacks, there is a dire need to manage such cyber risks proactively by predicting and protecting companies using AI technologies, such as expert systems, artificial neural network, intelligent agents and artificial immune systems. There are four categories (Early warning/ Prevent, Detect, Reach and Response) of possible scenarios where AI techniques are applied to security issues within the integrated security approach, demonstrating the vast possibilities of the various AI branches (Wirkuttis & Klein, 2017).

2. RESEARCH QUESTIONS

Cyber security or defence management is widespread across the research and corporate sectors. There are several studies regarding the utilisation of AI in cyber security functions throughout industries. The idea here is to address cyber risks through the application of AI as an emerging and/ or disruptive technology. The research may encompass a variety of AI technologies, such as artificial expert systems, neural networks, intelligent agents, and artificial immune systems, and how these technologies may change the cyber risk management landscape and their handling. This research addresses the following questions:

1. Does the knowledge acquisition problem affect the application of expert systems in decision-making or problem-solving in cyber security?
2. How do AI technologies such as neural networks help prevent cyberattacks proactively while managing the unknowns?
3. How do intelligent agents fight against cyber assaults such as Distributed Denial of Services (DDoS) and how effective are they?
4. How does an artificial immune system understand changes in patterns and report abnormal behaviour to detect intruders and mitigate risks related to cyber threats or vulnerabilities?

3. RESEARCH OBJECTIVES

In light of the research questions mentioned above, the following research objectives can be derived (also figuratively demonstrated below in Figure 1):