Chapter 4
Artificial Intelligence-Based Solutions for Cyber Security Problems

Merve Yildirim
Erzurum Technical University, Turkey

ABSTRACT

Due to its nature, cyber security is one of the fields that can benefit most from the techniques of artificial intelligence (AI). Under normal circumstances, it is difficult to write software to defend against cyber-attacks that are constantly developing and strengthening in network systems. By applying artificial intelligence techniques, software that can detect attacks and take precautions can be developed. In cases where traditional security systems are inadequate and slow, security applications developed with artificial intelligence techniques can provide better security against many complex cyber threats. Apart from being a good solution for cyber security problems, it also brings usage problems, legal risks, and concerns. This study focuses on how AI can help solve cyber security issues while discussing artificial intelligence threats and risks. This study also aims to present several AI-based techniques and to explain what these techniques can provide to solve problems in the field of cyber security.

INTRODUCTION

In the beginning, Artificial Intelligence (AI) emerged as a concept that mimics the human brain and tries to bring a human perspective and approach to the problems encountered. AI enables large amounts of data to be stored and intelligently processed with functional tools. AI has been widely used to create smart applications in a variety of fields, such as health, advertising, defense, industry 4.0, intelligent transportation systems, or space exploration. Cybersecurity systems are another critical area that AI mechanisms can be used for them to improve these systems.

AI can be defined as intelligence created to solve complicated and difficult problems in a computer or machine. It uses the combination of soft information technology and concrete human intelligence to solve problems. By recognizing artificial intelligence patterns, adaptive choices can be made, and the

DOI: 10.4018/978-1-7998-5101-1.ch004

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

ability to think by learning from experience can be provided. AI can briefly make machines behave like humans, but it performs much faster than them. These features of AI provide an important advantage in solving its cybersecurity problems.

Cybersecurity covers all of the technologies used to protect networks, data, computer software, and hardware from attacks and unauthorized access (Kaspersky Lab, 2018). Cybersecurity can also be called information technology security. It is a broad concept that includes many issues, from information security to end-user education. AI has a strong relationship with cybersecurity as cybersecurity is based on people's activities, organizational processes, and information technology (Vähäkainu and Lehto, 2019).

Organizations started using cybersecurity artificial intelligence to provide better information security against attackers who continuously improve their attack methods. Artificial intelligence helps to identify attacks and fight against information security breaches. As more cybersecurity attacks are specifically targeted to the networks every day, to address the challenge of defeating novel complex threats can be possible with using AI techniques. Cybersecurity practices are becoming more effective and comprehensive by using these techniques. Zero-day and multi-step attacks are among the most common attacks in the networks. Besides statistical analysis, machine learning can also be used to track these attacks in the AI field. Machine learning (ML) includes the detection of behavioral anomalies and event sequence tracking. Applications of AI involve online intrusion detection and offline security investigation. A recent study has provided a review of both statistical analysis and ML approaches to track some cyber-attacks which are hard to detect. They proposed a comprehensive framework for the study of detection and investigation of complex attacks. This work primarily facilitates the reduction of new complex threats by using AI-based countermeasures (Parrend et al., 2018).

Using AI for cybersecurity is for monitoring and analyzing the events that occur in a computer network to detect malicious activity that is mostly based on behavioral or signature. Therefore, most of the cybersecurity studies have focused on these fields. However, some traditional security mechanisms such as intrusion detection and prevention systems and Access control are not adequate to detect specific types of attacks, including zero-day threats. Because these types of attacks exhibit unknown misbehavior, which is not defined in the signatures' database of the cybersecurity systems. Recently, new cybersecurity mechanisms based on artificial intelligence (AI) have been developed to protect CPS from these zero-day attacks. Machine learning technologies are used to generate different types of attacks automatically, thereby managing a large amount of complex data from different sources of information to predict the wrong behavior of future attackers accurately. Game theoretical approaches have also been used in the context of cyber defense to solve whether the suspect device is an attacker and predict the attack. This approach is used to examine the interaction between security agents and competitors, such as IDS and IPS, to determine the optimal decision of security agents to classify or not classify the suspect opponent as an intruder.

This study discusses some artificial intelligence techniques which are suitable to be used in the cybersecurity domain. These can be used to predict and prevent information security threats and abnormalities. An overview of cybersecurity solutions using artificial intelligence and their capabilities and effectiveness is presented in this paper.

The aim of this study is mainly to highlight the shortcomings of traditional security measures and to demonstrate the progress made so far by applying AI techniques to cybersecurity. It reviews recent studies related to AI-based cybersecurity solutions applied to cyber-physical systems (CPSs). Most of these studies focus on AI-based cyber defense mechanisms to detect abnormalities in the network and attackers targeting CPS. The other studies investigate the cyber protection based solutions with machine

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/artificial-intelligence-based-solutions-for-cyber-security-problems/266133

Related Content

A Neutrosophic Intelligent System for Heart Disease Diagnosis: Case Study in Developing Country

Nouran M. Radwanand Wael K. Hanna (2022). *International Journal of Fuzzy System Applications (pp. 1-13).*

www.irma-international.org/article/a-neutrosophic-intelligent-system-for-heart-disease-diagnosis/302121

A Review of Systems Reliability Analysis Using Fuzzy Logic

Mohammad Abdolshah, Ali Samavi, Seyyed Amirmohammad Khatibiand Maryam Mamoolraftar (2019). *Advanced Fuzzy Logic Approaches in Engineering Science (pp. 362-377).*

www.irma-international.org/chapter/a-review-of-systems-reliability-analysis-using-fuzzy-logic/212343

Digital Transformation of Academic Libraries: Developments and Encounters

Raja T., Michael J. Leo A., Ramkumar R.and Anto Michael Suraj T. (2024). *AI-Assisted Library Reconstruction (pp. 307-328).*

www.irma-international.org/chapter/digital-transformation-of-academic-libraries/343593

The Affective Domain of E-Commerce

Vildan Ate (2020). *Advanced MIS and Digital Transformation for Increased Creativity and Innovation in Business (pp. 77-103).*

www.irma-international.org/chapter/the-affective-domain-of-e-commerce/237262

Application of Ambient Intelligence in Educational Institutions: Visions and Architectures

Vladimír Bureš, Petr Tuník, Peter Mikulecký, Karel Mlsand Petr Blecha (2016). *International Journal of Ambient Computing and Intelligence (pp. 94-120).*

www.irma-international.org/article/application-of-ambient-intelligence-in-educational-institutions/149276