UDC 004.8:004.7

ARTIFICIAL INTELLIGENCE SECURING IN CYBERSPACE

H. Sudani
Ministry of Higher Education and Scientific Research, Baghdad, Iraq

Abstract. Artificial Intelligence (AI) has become pivotal in enhancing cybersecurity measures across various sectors. By leveraging advanced techniques such as machine learning, deep learning, and natural language processing, AI systems can analyze vast amounts of data in real time to identify patterns indicative of potential threats. This capability enables the proactive detection and mitigation of cyber threats, including sophisticated attacks like phishing and malware intrusions. As cyber threats continue to evolve in complexity and frequency, the role of AI in fortifying cybersecurity defenses becomes increasingly indispensable. Fortunately, Artificial Intelligence (AI) technologies have been introduced into cyberspace to construct smart models for defending systems from attacks. Since AI technologies can rapidly evolve to address complex situations, they can be used as fundamental tools in the field of cybersecurity. In this paper, we review the impact of AI on cybersecurity.
Keywords: Artificial Intelligence; cybersecurity; Cyberspace; Threat Detection; cyberattack; machine learning; deep learning; natural language processing; computer network.

Introduction

The exponential growth of computer networks has led to a tremendous growth in several cyberattacks. All sectors of our society, from government to economy, to critical infrastructures, are largely dependent on computer networks and information technology solutions. Therefore, they are vulnerable to cyberattacks. A cyberattack is an attack launched from one or more computers against other computers or networks. Typically, cyberattacks

aim to disable the target computer, take the services offline, or get access to the target computer's data [1]. Since the first denial-of-service attack in 1988, the number and impact of cyberattacks have increased remarkably. Indeed, cybersecurity has become one of the most challenging tasks in the computer science field; and it is expected that the number and sophistication of cyberattacks will grow continually and exponentially. The exponential growth of computer networks has led to a tremendous growth in number of cyberattacks.

According to the definition provided by Myriam Dunn Cavelty [2]. Cybersecurity has become one of the most important issues in cyberspace [3, 4]. AI-driven solutions can effectively prevent phishing attacks by analyzing and recognizing malicious patterns in emails and websites. Moreover, AI enhances the efficiency of cybersecurity operations by automating routine tasks, allowing security professionals to focus on more complex issues. However, integrating AI into cybersecurity also presents challenges, such as the need to address potential biases in AI algorithms and the importance of maintaining ethical standards.

The role of AI in the field of cybersecurity

The convergence of AI and cybersecurity awareness can revolutionize threat detection, bolster response capabilities, and enhance user training. By leveraging AI's capabilities, organizations can enhance their cybersecurity measures to keep pace with the evolving threat landscape and mitigate risks effectively.

AI works in three ways:

1. Assistive intelligence, which improves on what people already do
2. Augmented intelligence, which allows people to do things they could not otherwise do.
3. Autonomous intelligence, which is the feature of machines acting on their own.

Concerning these three categories, it can be concluded that AI is aimed at solving some of the most complex problems and cybersecurity falls into this category as cyberattacks have become very complex and potentially more catastrophic and have become a complex problem in cyberspace. AI can be used in various areas of cyberspace to analyze data to detect and respond to attacks. AI can also automate processes, which helps security analysts quickly work with semi-automated systems to identify cyberattacks.

Artificial Intelligence in Threat Detection. AI-based security systems can monitor network traffic and user behavior to detect unusual activity. These systems can identify threats such as malware, ransomware, and phishing attacks. Unlike traditional methods that rely on predefined signatures, AI can learn from previous incidents and identify new types of threats, Table 1 shows the role of AI in threat detection.

Table 1. AI-Powered Threat Detection

AI Technology	Description	Example Use
Machine Learning	Identifies patterns in data to detect anomalies	Detecting new forms of malware
Natural Language Processing	Analyzes text and communication for suspicious patterns	Identifying phishing emails
Deep Learning	Advanced learning from vast datasets	Predicting zero-day attacks

AI for Intrusion Detection Systems (IDS). Intrusion detection is another area where AI plays a major role. Using AI, security systems can detect when an unauthorized user attempts to access a network and respond in real-time. AI models are continuously trained based on previous intrusion data to improve their detection capabilities, as described in Table 2. ML classification algorithms use indicator datasets to identify different malware behaviors in the datasets and classify them [5].

Table 2: Comparison of Traditional vs. AI-Enhanced IDS Performance.

Metric	**Traditional IDS**	**AI-Based IDS**
Accuracy	Medium	High
Detection Speed	Slow	Fast
Adaptability	Low	High
Cost	Higher Maintenance	Lower long term cost

As cyber threats continue to evolve, the role of AI will become even more important. The next generation of AI-powered cybersecurity systems will likely include more autonomous decision-making processes, where AI can not only detect but also mitigate threats in real time without human intervention.

Conclusions

The rapid growth of cyber threats and the sophistication of cyberattacks require new, more robust, flexible, and scalable methods. In current research, the main targets of AI-based algorithms for cybersecurity are malware detection, network intrusion detection, and phishing and spam detection. Various researchers leveraged a combination of different AI techniques, such as ML/DL methods together with bioinspired computation, or different learning methods such as supervised learning together with reinforcement learning. Such combinations yield outstanding results. Although the role of AI in solving cyberspace issues is inevitable, some problems related to trust in AI and AI-based threats and attacks would be another concern in the cyber environment. AI must also be continuously monitored and updated to ensure it remains effective in the ever-changing cybersecurity landscape.

References

1. Josh Fruhlinger,"Whatiscyberattack?,".CSO. February 2020https://www.csoonline.com/article/3237324/whatis-a-cyber-attack-recent-examples-showdisturbing-trends.html.

2. Cavelty, Myriam Dunn. "The Routledge Handbook of New Security Studies". 154-162. 2018.

3. Guan ZT, Li J, Wu LF, et al., "Achieving efficient and secure data acquisition for cloud-supported Internet of Things in smart grid". IEEE Internet Things J. 4(6): 1934-1944.

4. Wu J, Dong MX, Ota K, et al.,"Big data analysis-based secure cluster management for optimized control plane in software-defined networks.",IEEE Trans Netw Serv Manag. 15(1):27-38.

5. M. Rege, R. Blank, K. Mbah, "Machine learning for Cyber Defense and Attacks". The seventh international conference on data analytics. 2018.

Information about the authors

Sudani H., academic degree (Dr.Sci.(Eng)), academic rank(teacher), position (Head of the Department). Ministry of Higher Education and Scientific Research. info@mohesr.gov.iq.