

## **Investigating the Impact of Artificial Intelligence (AI) on Cyber Security**

Student Name: Badrul Alam

Course: Skills For Electronics

Institution: University of Wales

Date: 5/12/2023

# Investigating the Impact of Artificial Intelligence (AI) on Cyber Security

## Table of Contents

|                                                                        |   |
|------------------------------------------------------------------------|---|
| Abstract.....                                                          | 2 |
| Introduction.....                                                      | 2 |
| Objectives: .....                                                      | 3 |
| Research Questions or Gaps .....                                       | 3 |
| Literature review.....                                                 | 4 |
| Discussion and Findings .....                                          | 4 |
| Cybersecurity & AI Fundamentals .....                                  | 4 |
| Artificial intelligence (AI) .....                                     | 5 |
| The use of Artificial Intelligence in the field of cybersecurity ..... | 5 |
| Benefits of Using Artificial Intelligence in Cybersecurity .....       | 6 |
| Challenges of Using Artificial Intelligence in Cybersecurity:.....     | 6 |
| Conclusion .....                                                       | 7 |
| Bibliography .....                                                     | 7 |

## A. Abstract

The integration of Artificial Intelligence (AI) into the field of cybersecurity has become increasingly vital in the face of rising cyber threats and attacks. This study explores the current landscape of cybercrime and underscores the pivotal role of cybersecurity in the ever-evolving realm of information technology. Its primary objectives are to identify and evaluate potential applications of AI in bolstering cybersecurity, assess the associated risks linked to AI-powered cyberattacks, and formulate recommendations for harnessing AI's potential while mitigating these risks. AI, a multifaceted computer science application encompassing machine learning, deep

learning, and neural networks, aims to replicate human-like functionality. In the context of cybersecurity, AI proves to be a powerful ally. It excels at recognizing and countering cyber threats, enhancing detection systems, and enabling real-time responses. The advantages of AI in this domain include improved intrusion detection, reduced time consumption, more thorough risk assessment, superior cyber analytics, and proactive preparedness measures [2].

Nonetheless, the integration of AI into cybersecurity is not without its challenges, which range from the intricacies of implementation to potential issues and the necessity for further research. By incorporating AI into distributed systems, cybersecurity measures gain strength and efficiency. This leads to quicker responses to breaches and enhances the effectiveness of cyber analysts. As the prevalence and sophistication of malware and cyberattacks continue to grow, AI promises to be a crucial tool in fortifying our defenses against these evolving threats. This study sheds light on the symbiotic relationship between AI and cybersecurity, emphasizing its promise for a safer and more secure digital landscape.

**Key Words** (*Cybersecurity, Cybercrimes, Artificial Intelligence, Need for Artificial Intelligence in Cybersecurity, Artificial Intelligence Based Intrusion Detection Systems, Cybersecurity with Applications of Artificial Intelligence, Benefits & Challenges of Using Artificial Intelligence in Cybersecurity*)

## B. Introduction

Artificial intelligence (AI) is a compelling technology that can deliver

analytics and insight to safeguard against constantly developing cyberattacks [1]. AI can proactively predict and address potential issues by rapidly analyzing many events and monitoring diverse cyber threats. Kaur et al. [4] purport that due to this rationale, AI is progressively included in the cybersecurity framework and used in many scenarios to automate security operations or augment the efforts of human security personnel. The topic of cybersecurity has seen significant growth, attracting researchers from both the AI and cybersecurity domains. Consequently, several studies have been conducted to address various challenges associated with the identification, protection, detection, reaction, and recovery from cyberattacks.

The utilization of artificial intelligence (AI) in the field of cybersecurity has garnered significant interest within the information security community, particularly as machine learning (ML) algorithms continue to advance in complexity. Computer-based AI in cybersecurity is now being implemented or contemplated for various applications across several domains. Peters [5] suggests if a collective of individuals can accomplish a task, then it is plausible for AI to achieve the same, albeit potentially requiring some human intervention. The current period presents an exciting phase for individuals passionate about cybersecurity. To be well-informed about the latest developments in this field, one may use a corporate website such as Antivirus Rankings. Given recent data showing a significant increase in both the prevalence and sophistication of malware and cyberattacks, it is reasonable to anticipate that safeguarding against dangerous cyber threats will primarily involve sophisticated encryption techniques. The utilization of dispersed systems and the proliferation of cyber-attacks have intensified the imperative to prioritize cybersecurity.

Due to the escalating frequency and severity of cyber-attacks and viruses, there is a growing need for enhanced security measures. According to the source provided, artificial intelligence (AI) techniques and strategies can significantly bolster cybersecurity efforts, yielding highly successful outcomes. The primary objective of this study is to examine the current prevalence of cybercrime and the significant role cybersecurity plays in information technology during this era of technological advancement. Aside from that, this study looks into how artificial intelligence strategies might be used to strengthen cybersecurity measures and make it easier to build safer systems. This will open the door for more future research and progress in the field.

### **C. Objectives:**

The objectives of this project are to:

- Identify and assess the potential applications of Artificial Intelligence (AI) in cyber security.
- Identify and evaluate the potential risks associated with AI-powered cyberattacks.
- Develop recommendations for how AI can improve cyber security while mitigating the associated risks.

### **D. Research Questions or Gaps**

- How can AI be used to improve the efficiency and effectiveness of cybersecurity operations?
- What are the potential security risks associated with AI-powered cyberattacks?
- How can organizations mitigate the risks associated with AI-powered cyberattacks?

## **E. Literature review**

In their research, Abbas et al. [1] present findings on the rise of cybercrimes and attacks in India over the past decade. The number of instances involving wrongdoing resulting from cybercrimes has increased almost 30 times since 2010, even though only a few attacks lead to legal action.

The concept of artificial intelligence and its tactics were introduced by Noor et al. [2]. Moreover, the use of artificial intelligence and its associated applications can contribute to the prevention and mitigation of cybercrimes and attacks, enhancing the overall state of cybersecurity.

In his article, Peters [5], provided a comprehensive elucidation of the underlying concepts, key features, and practical applications of artificial intelligence (AI). Additionally, the person said that AI can help people do many mental tasks, such as thinking, planning, proposing, identifying, controlling, storing knowledge, being creative, and understanding new and important social facts.

Malatji et al. [3] examined 850 senior executives, scientists, and employees in the global information technology sector. The authors discussed contemporary challenges and cyber-related issues with senior executives, Chief Information Officers (CIOs), and Chief Information Security Officers (CISOs) across various enterprises. Furthermore, they conducted interviews with prominent figures in the industry and academia to examine the present state and impact of Artificial Intelligence (AI) in cybersecurity. The study discovered that the only application of artificial intelligence presently being made is to augment human

capacity in information and cybersecurity tasks; the trends for the future are still uncertain.

Kaur et al. [4] provided an overview and analysis of the benefits of integrating artificial intelligence (AI) with cybersecurity to enhance intrusion detection systems. Using a NIST cybersecurity framework and a thematic analysis approach, this article proposes a classification of AI use cases based on their applicability to cybersecurity provisioning and a systematic literature review of the relevant literature. This categorization scheme gives readers a bird's-eye view of AI's potential to enhance cybersecurity in various settings.

Noor et al. [2] study examines the impact of artificial intelligence on the security and detection systems of enterprises within the information technology sector. The association's investigation concludes that artificial intelligence is enhancing these systems. The user has provided a numerical reference without any accompanying text. The article notes many options for making systems stronger and more secure and proposes using AI for cybersecurity to solve this problem and create more reliable and secure systems. With its aim to demonstrate the current state of the art of applying AI techniques to cybersecurity, particularly in the fight against cybercrimes, the article shows that these methods can be a potent instrument for detecting and avoiding cybercrimes and ensuring better cybersecurity.

## **F. Discussion and Findings**

### **I. Cybersecurity & AI Fundamentals**

Currently, cybercrime is an area of criminal activity that is rapidly expanding. With technological advancement, individuals

increasingly rely on the Internet to fulfill their various demands. This is primarily due to its convenience in accessing shopping platforms, engaging in online gaming, doing internet searches, participating in social networking, and pursuing online job opportunities, among other activities, all inside a single digital space [1]. Various unlawful activities include a range of offenses, including but not limited to phishing, fraudulent activities using Visa and check cards, bank burglary, unauthorized downloading, child pornography, dissemination of computer viruses, and others.

**Malware Attack:** A malware attack uses harmful software by hackers or cyber-criminals to infiltrate a system for nefarious purposes [4].

**Phishing Attack:** Phishing attacks refer to a specific category of cyberattacks in which malicious actors assume false identities as representatives of reputable organizations or government entities to illicitly acquire an individual's confidential information, such as bank account numbers, ATM and credit card details, security PINs, passwords, and usernames [4]. Imposters of this kind pose a significant contemporary menace.

**Man-in-the-Middle Attack:** The man-in-the-middle attack occurs when two parties or entities directly communicate over a network, and an unauthorized individual infiltrates the conversation without the participant's awareness [1]. During data transmission, the cybercriminal intervenes and modifies the text or alters the intended meaning of the conversation.

## **II. Artificial intelligence (AI)**

Artificial intelligence (AI), an application of computer science, is popular and widely

used worldwide. In recent years, artificial intelligence has risen to popularity thanks largely to the numerous uses to which machine learning, deep learning, neural networks, and other similar techniques have been put. Yu et al. [6] state that these programs can employ deductive reasoning and acquire new skills using supervised, semi-supervised, and unsupervised study methods. They can also predict future events, such as the weather, or deal with potential challenges by identifying solutions that are likely to be effective. The goal of AI studies is to equip computers with brains as advanced as those of humans. There is still a long way to go until this milestone is reached, despite the incredible promise of AI.

## **III. The use of Artificial Intelligence in the field of cybersecurity**

The increasing prevalence of cybercrimes has necessitated the development of more robust, secure, and effective cybersecurity procedures. This need has led to the use of artificial intelligence tactics. Dai and Boroomand [7] purport that the use of artificial intelligence (AI) includes making intrusion detection systems that are strong and reliable, systems that change and act in smart ways, and systems that can adapt and learn [3]. This utilization of AI represents a remarkable achievement in the field. The integration of AI has the potential to enhance the security and reliability of systems, making it a compelling proposition. AI enables providing specific information from several angles. AI is widely used to identify cyber risks or hazards, leading to enhanced detection systems. These innovations demonstrate fresh capabilities. Machine learning or profound learning-based discovery enables associations to continuously improve identification bounds by employing social analysis to identify anomalies.

Unlike the successful implementation of artificial intelligence (AI) applications like spam filtering, numerous IT businesses and associations worldwide now use autonomous and semiautonomous cybersecurity measures. However, a potential concern arises if hackers and cyber-criminals begin using AI methods to maliciously target and breach legitimate systems and IT firms and associations. This might lead to various complications. Peters indicates [5] that it is essential to set up systems that can accurately predict, proactively avoid, and quickly respond to these high-level threats in real time to reduce the number of sophisticated attacks and threats.

Enhanced and Effective Response: Artificial intelligence (AI) and its applications have become more prevalent in contemporary businesses and associations. This is mainly because they can improve security using adaptive, learning, predictive, and dynamic intrusion detection systems. AI systems also provide enhanced efficiency in terms of reaction time, a critical factor for firms operating in the information technology (IT) sector [1]. These systems can resolve issues in real time.

#### **IV. Benefits of Using Artificial Intelligence in Cybersecurity**

The use of artificial intelligence (AI) in the field of cybersecurity has been recognized for its significant advantages. Due to the use of AI, it is possible for a group of humans—who may not necessarily number twelve—to complete this task without hurting the system's overall performance. Now, let us focus on certain advantageous elements of AI in cybersecurity [4].

- Intrusion detection and prevention measures exhibit enhanced efficacy and heightened security.
- This technology results in decreased time consumption and enhanced efficiency, facilitating quicker completion of organizational or individual tasks.
- Examining various risks may be facilitated by using learning capabilities, such as deep learning, which can potentially enhance a wide range of security applications.
- The use of cyber analytics leads to increased efficiency, particularly in the areas of threat research and detection.
- Implementing neural networks and intelligent agents facilitates predicting and comprehending future threats, enabling proactive preparedness measures.

#### **V. Challenges of Using Artificial Intelligence in Cybersecurity**

- The integration of artificial intelligence with cybersecurity is a multifaceted endeavor.
- The complexity of integrating, advancing, and using artificial intelligence in conjunction with cybersecurity poses challenges.
- The process of resolving any potential issues that may occur might be challenging.
- Understanding these ideas might be challenging for those new to the technical field.
- Substantial future work remains to be undertaken on this particular subject.

## G. Conclusion

This study investigated the optimal uses of artificial intelligence (AI) in addressing cybersecurity challenges. Integrating AI with reasoning and intuition has been recognized as a valuable approach to enhancing cybersecurity measures. This advancement has the potential to fortify both contemporary technological systems and human decision-making processes. When we collaborate, we can develop highly effective and enhanced technologies, such as improved detection technologies, autonomous and semiautonomous cybersecurity, autonomous cyber defense, efficient and enhanced response, and predictive analytics for security [3]. Moreover, the integration of AI in distributed systems enhances the level of protection and security. This integration also enables organizations to respond more swiftly to breaches and improves the efficiency of cyber analysts. Consequently, the utilization of AI in conjunction with cybersecurity proves advantageous.

## F. Bibliography

- [1] N. N. Abbas, T. Ahmed, S. H. U. Shah, M. Omar, and H. W. Park, "Investigating the applications of artificial intelligence in cyber security," *Scientometrics*, vol. 121, no. 2, pp. 1189–1211, Sep. 2019, doi: <https://doi.org/10.1007/s11192-019-03222-9>.
- [2] A. Noor, T. Nafis, S. Wazir, and M. Sarfraz, "Impact Of Artificial Intelligence In Robust & Secure Cybersecurity Systems: A Review," *SSRN Electronic Journal*, 2021, doi: <https://doi.org/10.2139/ssrn.3834207>.
- [3] M. Malatji, A. Marnewick, and S. von Solms, *Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018)*. Lulu.com, 2018. Accessed: Nov. 03, 2023. [Online]. Available: <https://books.google.com/books?hl=en&lr=&id=XXRvDwAAQBAJ&oi=fnd&pg=PA158&dq=S.+von+Solms>
- [4] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions," *Information Fusion*, vol. 97, p. 101804, Apr. 2023, doi: <https://doi.org/10.1016/j.inffus.2023.101804>.
- [5] K. M. Peters, "21st Century Crime: How Malicious Artificial Intelligence will Impact Homeland Security," *apps.dtic.mil*, Mar. 01, 2019, <https://apps.dtic.mil/sti/citations/AD1073657>
- [6] Y. Xu *et al.*, "Artificial Intelligence: A Powerful Paradigm for Scientific Research," *The Innovation*, vol. 2, no. 4, p. 100179, 2021, doi: <https://doi.org/10.1016/j.xinn.2021.100179>.
- [7] D. Dai and S. Boroomand, "A Review of Artificial Intelligence to Enhance the Security of Big Data Systems: State-of-Art, Methodologies, Applications, and Challenges," *Archives of Computational Methods in Engineering*, Jul. 2021, doi: <https://doi.org/10.1007/s11831-021-09628-0>.

