ISSN NO: 2770-4491
Date of Publication:26-03-2023

The Influence and Limitations of AI in Cybersecurity Domain

Ikromjon Tojiboyev
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan
Nuriddin Safoev
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan

Abstract: The use of artificial intelligence (AI) is creating new opportunities for creating value in businesses, industries, communities, and society as a whole. As technology has become increasingly relevant in many aspects of the world, it has been integrated into various industries, including cybersecurity. With the growing importance of information technology in businesses, cybersecurity has become crucial to protect data and information. AI has been heavily influencing cybersecurity on a large scale, and machine learning has been increasingly used in recent technologies supporting cybersecurity. This research paper reviews literature on the impact of AI on cybersecurity.

Keywords: Cybersecurity, AI, Machine learning, Threats, Limitations**.**

I. Introduction

The development of artificial intelligence (AI) dates back to the 20th century when researchers were trying to create a system that could function without the assistance of a human brain. This discovery led to further research on developing intelligent systems and robots that could mimic human behavior without affecting humans significantly. Mathematicians also contributed to this field by developing formulas to aid in the process. Organizations invested heavily in these studies, and AI has since come a long way. Today, AI platforms help enterprises in developing, managing, and deploying machine learning and deep learning models at scale, reducing software development tasks such as data management and deployment, making AI technology more accessible and affordable. With the increase in cyber risks, AI is also being employed to monitor and restrict cybercrime.

II. Related Works

The advancement of computers and processing units has facilitated the remarkable growth of AI. It is evident from the graph that people have recognized the potential of AI since its inception. Algorithms have continued to develop with each generation of computers, and countries have competed to be at the forefront of this technology. This competition has fueled the extensive growth of AI. There was a significant surge in AI technology at the end of the 20th century, during which its true power and significance were realized. Further research has led to the discovery of more applications for the technology. Figure 1 below provides a detailed illustration of the AI life cycle [1].

ISSN NO: 2770-4491
Date of Publication:26-03-2023

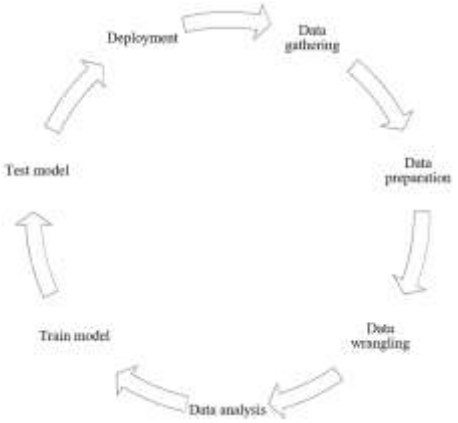

Figure 1. Life-cycle of AI.

It is evident that artificial intelligence has experienced significant growth, and vast amounts of data have been collected over the years for accurate analysis and predictions. These attributes have greatly influenced the integration of AI in various industries and organizations, benefiting initiatives such as banking, marketing, and entertainment. Computers can model human actions and reactions, and robots that mimic human behavior have been developed. Personal assistant applications and devices have also seen a rise in popularity, such as Alexa and Siri, while others like Google Assistant have proven to be efficient in assisting people. Figure 2 below illustrates some of the applications of AI, showcasing its overall impact on various technologies.

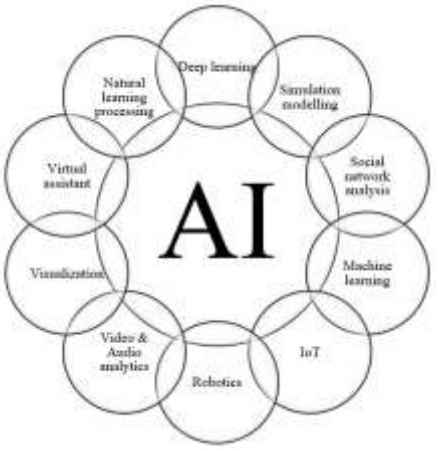

Figure 2. Artificial Intelligence areas.

As previously mentioned, artificial intelligence has numerous applications across various industries and sectors. One such sector that has benefited significantly from AI is cybersecurity, and its specific impacts are discussed in the following study. The field of cybersecurity involves protecting computer systems and other devices from attacks, most of which occur over the Internet, resulting in significant resource loss for organizations [2, 3]. According to [4], cyber-attacks are becoming the new form of terrorism, posing a threat to countries. Recent technological advancements have demonstrated that businesses can be destroyed by a single attack, and [5] define cybersecurity as protecting computer systems from Internet-based attacks. Organizations must implement strategies to safeguard their information as competitors may launch attacks to gain an advantage. Confidential and private information requires extra measures to ensure its protection, ensuring the safety of people and organizations.

ISSN NO: 2770-4491
Date of Publication:26-03-2023

Figure 3. Cybersecurity threats.

The field of cybersecurity has been categorized into different units to ensure the privacy and security of both individuals and companies. These categories include application, network, information, and operational security, which are crucial in achieving the benefits of cybersecurity and promoting business continuity and development. As shown in Figure 3, various threats affect cybersecurity, making it necessary for individuals to protect their information. To achieve this, several methods are being developed and improved regularly, including the use of artificial intelligence. According to [6], the recent successes of artificial intelligence in cybersecurity have resulted in significant data advantages, with machine learning technology being used to avoid potential threats to company data and information. Therefore, artificial intelligence has had a significant impact on cybersecurity, which will be further discussed below.

III. The Influence of AI on Cybersecurity

The integration of AI technology globally has resulted in various impacts, both positive and negative. The development of technology has been significant across different industries, including cybersecurity, which has benefited all sectors [7]. According to [8], businesses and companies have been influenced by AI technology. However, the overall effects of AI on cybersecurity are mixed. Companies face increasingly dangerous attacks, as attackers become more knowledgeable in finding weaknesses in cybersecurity technologies. Nonetheless, the automation resulting from machine learning algorithms has prevented attackers from using the same methods to attack systems with AI. The technology has also shown that machine learning algorithms are better at providing security than humans. The integration of AI into cybersecurity helps to prevent errors, which is one of the various benefits of AI on cybersecurity that are discussed below.

Artificial intelligence (AI) technologies play various roles in ensuring cybersecurity [9, 10] and are constantly being researched to improve their efficiency in preventing attacks. As mentioned earlier, organizations worldwide require confidential information to be protected, and AI technologies must ensure that unauthorized access is prevented. The future of AI in cybersecurity is expected to incorporate larger-scale developments to enhance security in organizations. Many companies envision systems that can protect themselves and detect any attempts at breach, and achieving such a level of security is a goal that researchers and IT companies are striving to accomplish. One of the crucial features of AI integration in systems is the ability to learn from experience, a fundamental characteristic of AI. The technology has demonstrated that systems can learn from past events, which is crucial in enhancing cybersecurity [11]. AI is considered a rescue technology in cybersecurity because it can learn from experiences and detect potential threats before they can cause any damage [12]. AI algorithms have been utilized in cybersecurity technologies and algorithms to prevent previous mistakes from recurring. Consequently, attacks are embedded in a system where AI algorithms can detect and learn from them to enhance security.

AI technology is considered one of the most advanced technologies available today. Its ability to accomplish tasks without limitations and errors has been a great attraction for developers. Every organization that adopts AI technology guarantees increased efficiency and improved services. Additionally, AI technology has been instrumental in reducing cybercrimes, which is a major problem in the modern world.

ISSN NO: 2770-4491
Date of Publication:26-03-2023

The technology has the capability of detecting and addressing these activities, making it more effective than human monitoring. This feature is essential in ensuring technological security in the world today. Real-time traffic monitoring enables AI technology to detect any unauthorized activity and act on it immediately. The system ensures that it deals with the issue before it becomes too late, thus safeguarding the organization's data and information. Furthermore, this helps the organization to enhance its security protocols and make necessary improvements. In general, AI technology has made a significant impact on the security of organizations and their operations.

AI technology has played a crucial role in enhancing data security measures and protocols. Business organizations highly value their data and require that it is protected [13]. The system can achieve significant encryption with the aid of various data encryption protocols, which guarantees the safety of the data involved. The use of strong protocols has significantly influenced the impact of AI technology in the cybersecurity sector [15]. The implementation of AI technology in the field of cybersecurity has led to some job displacement, as the computer's superior efficiency has made it a preferred choice over human cybersecurity specialists. The introduction of AI has also reduced the need for maintenance and check-ups on the system, as the technology is highly efficient in securing security protocols [14]. Organizations that have implemented AI technology in their systems have experienced improved efficiency and security of their data, as the technology continues to learn and understand the operations of the system.

According to [14], the integration of learning-based artificial intelligence systems in cybersecurity aids in preventing attacks on a system. The system learns from the actions of attackers and adapts to protect the information, making it impossible for them to gain access to the data. This learning capability is one of the features that has made the technology highly effective. AI has been successful in thwarting cyber-attacks through various techniques, which have ensured the efficiency of AI in the field of cybersecurity.

AI has had a significant impact on cybersecurity through signature-based techniques, which involve the detection of cyberattacks and malware through codes. This has been a critical attribute of AI technology in cybersecurity. Using an AI algorithm, these codes in the malware or attacks can be detected, and then compared to signature codes from recent attacks or a database to stop the attack [16]. Quick comparison of signatures is necessary to detect the attack, which helps provide time and resources needed to halt the attack. Before AI technology was integrated into cybersecurity, the detection of these attacks would take a lot of time, leading to significant failures and losses.

The advanced technology of AI has greatly impacted the cybersecurity field, with signature-based techniques being one of the most critical attributes. These techniques involve detecting cyberattacks and malware through codes using AI algorithms. The codes are matched with signatures stored in a database called a blacklist, which is used to compare and identify the attack. Although this method has proven to be efficient, it fails when dealing with new attacks since the database has no record of the attack. Hackers can also evade this technique by altering their patterns to avoid detection. Despite its limitations, the technique has been able to prevent numerous attacks. The applications of AI in cybersecurity are illustrated in Figure 4.

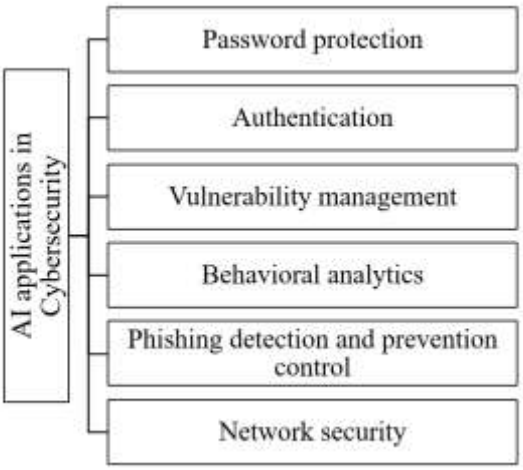

Figure 4. Application of AI in cybersecurity.

ISSN NO: 2770-4491
Date of Publication:26-03-2023

The impact of machine-based learning on cybersecurity has been significant, as pointed out earlier. One of the advantages of AI technology is its ability to avoid errors and omissions that humans tend to make while analyzing data or information. This advantage ensures that attacks are quickly detected through AI analysis of logs and network packets, allowing system administrators to change access permissions and prevent further loss. AI technology is often compared to human analysts due to its efficiency in detecting and preventing attacks.

The most significant advantage of AI in cybersecurity is its ability to analyze large amounts of data accurately. This was a tiring task for human analysts before the advent of AI technology. With AI, large volumes of data can be analyzed without error. Human analysts also play a crucial role in detecting attacks by working alongside the AI system. By combining their efforts, all available data is analyzed and compared, resulting in efficient attack prevention. The first step in preventing attacks and protecting data is identifying malware. Machine learning systems use techniques such as classification and clustering to compare available information with logs, detecting errors and infected logs. Clustering groups available information to detect anomalies, and both techniques have proven effective in detecting attacks, which is impossible for humans to achieve.

Cybersecurity is heavily impacted by network attacks, which are frequently used by attackers to infiltrate organizations and companies. Detecting network attacks is crucial in order to prevent them from causing harm. Fortunately, AI has made this task much easier by embedding the technology in network firewalls, making it more difficult to gain unauthorized access. Preventing attacks from the web is the first step in safeguarding sensitive information, and this approach has proven to be effective in preventing future attacks. Network intrusion detection systems are also equipped with five elements that ensure the full security of networks. The first element is the ability of AI systems to analyze large amounts of data from the network, which is critical in protecting the network from potential threats. AI technology has been instrumental in teaching systems how to avoid attacks and ensure the network remains uncompromised. This is just one example of how AI has significantly impacted cybersecurity at a network level, with various techniques and approaches contributing to increased security measures.

The management of vulnerabilities in an organization's system can be a challenging task for human personnel, which is why artificial intelligence machines have been introduced to handle this task. This approach has proven to be an effective way of preventing hackers from gaining unauthorized access to systems, and it is one of the many benefits of AI on cybersecurity. In the past, hackers would exploit the slow reaction of vulnerability management systems to launch attacks, but the inclusion of AI has changed this dynamic. With AI systems managing the vulnerability database, potential attack attempts can be quickly identified and reported, leading to safer systems. Additionally, machine learning algorithms can detect user account anomalies, providing an added layer of protection to the system in case a user becomes a threat. Overall, vulnerability management by AI systems has made servers and the information stored on them much safer.

As previously discussed, protecting data from cyber-attacks is a crucial aspect of cyber security. AI has been implemented to enhance security and efficiency in this area. In particular, data centers are of utmost importance in terms of cyber security, and AI has proven effective in automating processes and managing critical aspects such as power consumption, bandwidth usage, and temperature control. This is because human errors can lead to vulnerabilities in the data center's security.

Additionally, hardware maintenance costs are a critical factor in data centers, and AI systems can help ensure the machines are safe from environmental threats. As a result, more companies and organizations are adopting AI systems in their data centers to improve security and efficiency. This demonstrates the significant impact of AI on cyber security. However, despite its benefits, AI also has limitations in cyber security.

IV. AI Limitations in Cybersecurity

The use of computer technology has become ubiquitous in today's world, and it supports many crucial aspects of our lives. As a result, it is essential to implement standards to ensure the efficiency and security of the services provided. This technology is used by financial institutions and other sectors that hold sensitive information about our lives, as well as information about organizations that could be used to gain a competitive advantage. In light of how critical information is in today's world, computer technicians and developers must

ISSN NO: 2770-4491
Date of Publication:26-03-2023

ensure that all security protocols are in place to protect the data involved in the system. To ensure data security, computer scientists developed data encryption protocols that encrypt the data before sending it. The encryption protocol makes it difficult for unauthorized individuals to use the data without a decryption code [17]. Over time, people have become more familiar with the principles behind data encryption, and this has led to the development of business process barriers and encryption protocols as hurdles to using AI in various organizational challenges, including cybersecurity threats, to create value.

The prevalence of computer technology in modern society has led to the development of encryption systems and protocols to ensure data security. However, as people learned about the encryption protocols used by these systems, they became easier to reverse engineer, posing a security threat. To address this issue, computer scientists developed more complex protocols and methods for encrypting data. With the increasing role of machines in security, artificial intelligence (AI) has been introduced to improve data security. AI technology uses various data encryption protocols to ensure that it is difficult to decode data involved in transactions. While AI has improved data security, it is limited by its programmed nature, which means it can be manipulated and used as a weapon by those with the appropriate knowledge. Nonetheless, AI can be trained to detect cyber threats and malicious malware, making it more effective in cybersecurity. However, AI is not a complete replacement for humans in cybersecurity as it can struggle with evolving threats and requires human expertise for creativity. To address these limitations, developers must equip AI technology with multiple capabilities to handle any cybersecurity threats resulting from these limitations.

V. Conclusion

The impact of AI technology on various industries includes both its benefits and limitations. However, when it comes to cyber security, the benefits of AI outweigh its limitations. As AI technology continues to grow, ongoing research and development are helping to advance it further. The use of AI in cyber security has resulted in significant improvements in security measures. However, there are still some limitations to AI that can be exploited by individuals for personal gain, leading to constraints in cyber security. To address this issue, researchers and innovators should work to create more secure systems using AI technology. Enhancing cybersecurity measures will prevent attackers from exploiting organizations, leading to further growth and development of companies. Overall, the impact of AI technology on cyber security has been substantial, with AI playing a significant role in improving security measures.

Reference

1. Álvarez López, José Antonio. “Case Studies of Real AI Applications.” Artificial Intelligence for Business: Innovation, Tools and Practices. Cham: Springer International Publishing, 2022. 141-157.
2. Kuzlu, Murat, Corinne Fair, and Ozgur Guler. “Role of artificial intelligence in the Internet of Things (IoT) cybersecurity.” *Discover Internet of things* 1 (2021): 1-14.
3. Kaloudi, Nektaria, and Jingyue Li. “The ai-based cyber threat landscape: A survey.” *ACM Computing Surveys (CSUR)* 53.1 (2020): 1-34.
4. Stevens, Tim. “Knowledge in the grey zone: AI and cybersecurity.” *Digital War* 1 (2020): 164-170.
5. Trappe, W., and J. Straub. “Cybersecurity: A New Open Access Journal. Cybersecurity, 1 (1), 1.” (2018).
6. Stoianov, Nikolai, and Andrey Ivanov. “Public Key Generation Principles Impact Cybersecurity.” *Information & Security* 47.2 (2020): 249-260.
7. Vlassis, Nikos. “A concise introduction to multiagent systems and distributed artificial intelligence.” *Synthesis Lectures on Artificial Intelligence and Machine Learning* 1.1 (2007): 1-71.
8. Perols, R. R., and U. S. Murthy. “The impact of cybersecurity risk management examinations and cybersecurity incidents on investor perceptions.” *SSRN Electronic Journal. https://doi. org/10.2139/ssrn* 3112872 (2018).
9. Hamilton, William L. “Graph representation learning.” *Synthesis Lectures on Artifical Intelligence and Machine Learning* 14.3 (2020): 1-159.
10. Wood, Trevor, et al. “Systematic Literature Review: Anti-Phishing Defences and Their Application to Before-the-click Phishing Email Detection.” *arXiv preprint arXiv:2204.13054* (2022).
11. Szepesvári, Csaba. “Algorithms for reinforcement learning.” *Synthesis lectures on artificial intelligence and machine learning* 4.1 (2010): 1-103.

ISSN NO: 2770-4491
Date of Publication:26-03-2023

12. Truong, Thanh Cong, et al. "Artificial intelligence and cybersecurity: Past, presence, and future." *Artificial intelligence and evolutionary computations in engineering systems*. Springer Singapore, 2020.
13. De Raedt, Luc, et al. "Statistical relational artificial intelligence: logic, probability and computation." (2017).
14. Mengidis, Notis, et al. "Blockchain and AI for the next generation energy grids: cybersecurity challenges and opportunities." *Information & Security* 43.1 (2019): 21-33.
15. Raghavan, Vijay V., et al. *Cognitive computing: Theory and applications*. Elsevier, 2016.
16. Marda, Vidushi. "Artificial intelligence policy in India: a framework for engaging the limits of data-driven decision-making." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376.2133 (2018): 20180087.
17. Qasaimeh, Ghazi M., and Hussam Eddin Jaradeh. "The impact of artificial intelligence on the effective applying of cyber governance in jordanian commercial banks." *International Journal of Technology, Innovation and Management (IJTIM)* 2.1 (2022).