International Journal of Computer and Organization Trends
ISSN: 2249 – 2593 / https://doi.org/10.14445/22492593/IJCOT-V12I2P302
Volume 12 Issue 2, 6-8, May-Aug 2022

Original Article

Use of AI in Cybersecurity Applications toward Advanced Defensive Security Discipline

Alex Mathew

Department of Cybersecurity& Bethany College, USA

Received: 14 April 2022 Revised: 11 June 2022 Accepted:17 July 2022 Published: 04 August 2022

Abstract *- Based on the technological developments in the world and the increased risk of cyber-attacks, utilizing the most recent technology to achieve security is necessary. Identifying the threat can be challenging, and several methods and algorithms have been suggested, including reinforcement, supervised, and unsupervised learning. The strategic plan for implementing AI includes the automation of available infrastructure to ensure that the available labor resources are utilized efficiently. Additionally, running the IT infrastructure on a 24-hour basis seals loopholes that can be used to compromise the integrity of the entire system. Time and physical resources are required to smoothen the process of AI implementation. Additionally, defense tactics can be used, including model alteration, change data, and support resources. Consequently, it is important to look at the technical approach that can be used to incorporate AI into the cyber defense system.*

Keywords *- Cybersecurity, Technology, Algorithm, Defense, Artificial intelligence (AI).*

1. Introduction

Artificial intelligence refers to the simulation of human activities by a machine. On the other hand, cybersecurity refers to the use of technology, people, and processes to protect organizations, sensitive information, critical systems, and digital tasks [1]. Most of the threats to which computer systems are exposed are from online sources. For this reason, AI is one of the tools that can help build a defense system. There are several ways through which AI can be utilized in cyber defense systems. For instance, it can detect vulnerable areas and conduct automatic responses, such as self-patching. There are also called self-configuring networks. The current technological advancements make it difficult to know which innovation to adopt. Resource-intensive efforts have dominated the world of cyber security. Some activities performed during routine cybersecurity check-ups include threat hunting and monitoring. Notably, these activities can be time intensive and could delay action that leads to exposure to harm and increase the vulnerability to cyber adversaries. The continued maturity of AI has increased substantially to the extent that it provides substantial benefits to defensive operations across a range of missions and organizations. Automating key functions of the AI system can greatly increase computer systems' security, reliability, and cyber workflows. For this reason, it is important to come up with a technical approach that can be used to incorporate AI as a cyber-defense system.

2. Proposed Methodology Block Diagram

2.1. Increasing Automation

The value of harnessing cybersecurity with AI is becoming vivid with its continued technological advancement leading to more capabilities in the defense systems. AI technologies possess the capability to generate signals during the attack, adaptive responses, and effective prioritization of threats. AI shows great promise in analyzing and correlating patterns across numerous points to track any cyber threats within seconds [2]. Notably, AI can learn new methods and adopt new strategies learned through insights and past observations. As such, AI promises to prevent future attacks through machine learning.

The plan for advancing defense cybersecurity through AI is to increase the automation power of the available infrastructure. The current workforce gap can be breached using AI and ease the burden on the experts in this discipline [3]. It is also important to appreciate a global shortage of cybersecurity professionals. To have an effective management program for cybersecurity, most corporations with the capacity need to run a 24/7 operation. The shortage of skilled IT personnel who can handle such issues should be addressed by introducing the AI system to speed things up and ensure timely responses to threats.

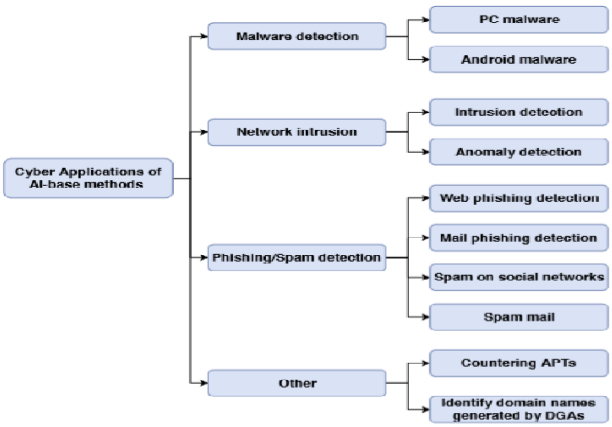

Fig. 1 AI intervention.

2.2. Improving Defense System

The next step in improving defense security in cybersecurity using AI is allowing defenders to scale their capabilities efficiently. This will involve automating tasks

that require a lot of time to perform. Actions that require executing complex algorithms should also be automated by applying AI. Some of the activities may be repetitive may and require complicated response actions. The beauty of AI systems is that they can handle large volumes of threats with minimal human interventions and deliver better results.

2.3. Improving Training

The next step is to improve the training of cybersecurity experts so that they are in a position to handle AI effectively. It could include training on how to incorporate AI at various stages of security. The defense process can occur in multiple stages, including classification and discovery, detection, prevention, investigation, and remediation [4]. The ability of AI to gather cyber intelligence will automatically open up defensive applications at the operational and tactical levels of cybersecurity. AI could be used to retrieve and process data obtained from network security analysis programs and obtain correlations with other valuable data. AI will be a tactical tool for detecting threats, prevention, and analysis. It will be achieved by upgrading the intrusion Detection system that aims to unveil the illicit activities in a network. Another application of tactical defense using AI is the process of automating vulnerability testing. This process is also called fuzzing. False positives and negatives taint this process. However, this process requires the development of unique biometric passwords, the ability to detect risks and suspicious activity, the ability to think and interpret speech, and a method of securing identification. Adding AI into the system will require time.

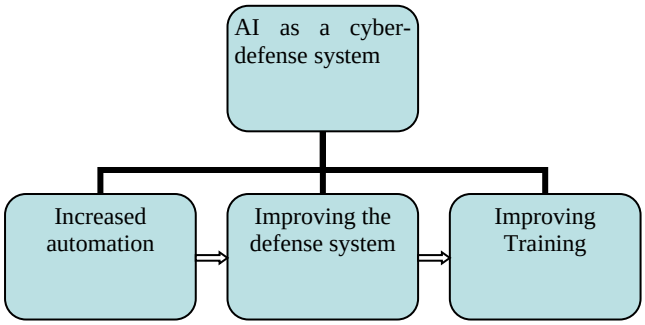

Fig. 2 Proposed methodology diagram.

3. Algorithm

AI is a type of intelligence that seeks to provide an automatic response that can be likened to human intelligence. For this goal to be achieved, machines will need to have the capacity to learn. Notably, training requires training that relies on learning algorithms [5]. Generally, the learning algorithm will aid in ensuring that AI's performance is exceptional. Data from previous incidents is used to further the learning process and improve future responses [7]. Three algorithms can be used to imagine training: supervised, unsupervised, and reinforcement learning.

Supervised learning requires a process that utilizes previously labeled data. These algorithms are mainly used as a mechanism of classification or regression. Unsupervised learning methods utilize unlabeled datasets. This approach is mainly suitable for clustering data, estimating density, and reducing dimensionality. On the other hand, reinforcement learning is another algorithm that assumes the best lessons based on punishment and reward. Reinforcement learning also uses simulations in cases where data is limited or has not been issued. Notably, learning methodologies are defined by neural networks and an evolutionary algorithm.

4. Flow chart

Several benefits can be obtained by using AI in defense cybersecurity systems. In a broad category, some AI applications are in malware detection, network intrusion, and spam/phishing detection, among others. One of the most central functions of AI is identifying malicious programs. According to the creators of smart malware detection programs, AI has the potential to run programs that will effectively identify any malware. It is based on developing various applications like CNN, ANN, and DAE [7]. The other intervention is the detection of interruption. It is a framework that aims at shielding against incidents of violation or danger. The third application is in SPAM phishing and detection. The phishing assault aimed to take the client's monetary certifications or character. Machine learning and AI software will also need to be applied [8]. Generally, these are some techniques that can be applied through AI to improve the defense process for cyber systems.

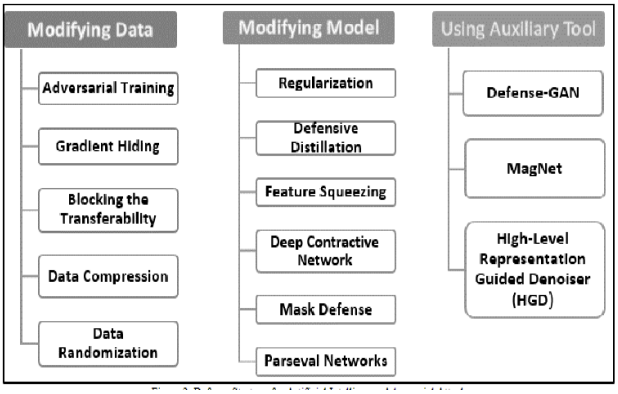

Fig. 3 Cybersecurity Tactics

Three major defined tactics can be applied in the cybersecurity initiative: model alteration, change, data, and support resources. Some of the data modification techniques that were found to be effective in the process of defense using AI involved data testing, preventing infiltration, compression of data concealed gradient rates, pseudo-random data, and compression of data [9]. For this reason, there is a chance that the compression of data has the potential to limit vulnerability [14]. On the other hand, the updated model is another strategy that can be employed to protect data. Pattern recognition models can be altered, including regularization and mask safety. This approach can be effective because it involves the insertion of penalty limits in the cost function, which will make the attacks

predictable. An auxiliary tool is a technique that applies eternal methods as a supplementary method for the neural network template. Defense GAN has demonstrated its effectiveness in protecting against attacks. Notably, it relies on relational efficacy and expressiveness.

5. Results analysis

Artificial intelligence can potentially transform the informational security sector significantly [11]. Numerous attacks on defense, governments, and technology companies or financial crimes have run costs in millions of dollars. Based on the technological advancements presented earlier, it is impossible to identify the role of AI in defense and cybersecurity. Defense is crucial for government infrastructure and nationwide security. Operating with minimally effective mechanisms and overlying on the already inadequate IT labor tool is an ineffective strategy in handling cybersecurity issues.

There are many benefits that the incorporation of AI in defense cybersecurity will yield. For instance, the protection and remediation of AI due to heightened security, nuanced attacks, and enhanced incident response are some of the results that are expected. Automation will increase the speed at which attacks are responded to and improve the defense levels for technological assets. Notably, AI was found to have a high chance of success in detecting attack techniques [12]. Despite the increasing cyber-attacks, AI presents a lasting defense option for many companies and organizations, including governments. AI has the potential to provide a more efficient, reliable, and fast system that offers a clear advantage in web security and penetration.

Countries that are cyber-dependent are at risk of manipulation through attacks. As indicated earlier, modifying data will require blocking transferability, data randomization and compression, gradient hiding, and adversarial training. On the other hand, modifying models includes defense distillation, regularization, feature squeezing, deep construction network, personal networks, and mask defense. Finally, the auxiliary tool performs defense-GAN and MagNet.

6. Conclusion

AI offers a range of advantages for defense against cybersecurity threats. Some of the retreats that exist through online platforms can affect institutions, governments, financial bodies, or other entities that have an online presence. These could be banks, hospitals, or even IT companies. AI offers numerous advantages in intensifying security in digital space. Some of the advantages associated with AI are the ability to respond fast to threats and process huge chunks of data that may not be humanly possible.

Moreover, the AI system can operate routine tasks, including eliminating potential threat sources. For this reason, implementing an AI defense system will require the right equipment and skills. Notably, having an AI system in the defense system for cybersecurity is more advantageous.

References

[1] R. Das and R. Sandhane, "Artificial Intelligence in Cyber Security," *Journal of Physics: Conference Series*, Vol. *1964*, 2021.

[2] M. E. Bonfanti, *Artificial Intelligence and Cybersecurity: A Promising But Uncertain Future*, 2020. [Online]. Available: Https://Www.Realinstitutoelcano.Org/En/Analyses/Artificial-Intelligence-and-Cybersecurity-A-Promising-But-Uncertain-Future/

[3] T. C. Truong, Q. B. Diep, and I. Zelinka, "Artificial Intelligence in the Cyber Domain: Offense and Defense," *Symmetry*, Vol. 12, Pp. 410, 2020.

[4] A. H. Althobyti, S. M. Alhusayni, and S. M. Alzahran, "Defense By Artificial Intelligence in Cyber Attack," *International Journal of Scientific Engineering and Science*, Vol. 5, Pp. 35-40, 2021.

[5] B. Herron, "Implementing Security Controls to Iot Wireless Technologies," *Giac (Gccc) Gold Certification*, 2022.

[6] M. Raney, "Threat Hunting: This Is the Way," *Giac (Gccc) Gold Certification*, Pp.1-22, 2021.

[7] J. Li, "Cyber Security Meets Artificial Intelligence: A Survey," *Frontiers of Information Technology & Electronic Engineering*, Vol. 19, Pp. 1462-1474, 2018.

[8] F. Kamoun, F. Iqbal, M. A. Esseghir, and T. Baker, "Ai and Machine Learning: A Mixed Blessing for Cybersecurity," *2020 International Symposium on Networks, Computers and Communications (Isncc)*, 2020.

[9] C. Benzaid, and T Taleb, "Ai for Beyond 5g Networks: A Cyber-Security Defense Or Offense Enabler?" *Ieee Network*, Vol. 34, Pp. 140-147, 2020.

[10] Evans Mwasiaji, Kenneth Iloka, "Cyber Security Concerns and Competitiveness for Selected Medium Scale Manufacturing Enterprises in the Context of Covid-19 Pandemic in Kenya," *Ssrg International Journal of Computer Science and Engineering*, Vol.8, No.8, Pp.1-7 2021. Crossref,Https://Doi.Org/10.14445/23488387/Ijcse-V8i8p101

[11] J. Johnson, "Artificial Intelligence & Future Warfare: Implications for International Security," *Defense & Security Analysis*, Vol. 35, Pp. 147-169, 2019.

[12] D. Ventre, "Artificial Intelligence and Defense Issues," *Artificial Intelligence, Cybersecurity and Cyber Defense*, Pp.105-186, 2020.

[13] S. Gavaskar, E. Ramaraj, R. Surendiran, "A Compressed Anti Ip Spoofing Mechanism Using Cryptography," Ijcsns International Journal of Computer Science and Network Security, Vol. 12, No. 11, Pp.137-140, 2012.

[14] Booz Allen Hamilton, *The Role of Artificial Intelligence in Cybersecurity*, 2021. [Online]. Available: Https://Www.Boozallen.Com/S/Insight/Publication/Role-of-Artificial-Intelligence-in-Cyber-Security.Html.