International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

# AI and Cybersecurity - How AI Augments Cybersecurity Posture of an Enterprise

**Suresh Babu Rajasekaran**

**Submitted:** 25/10/2022 **Revised:** 02/12/2022 **Accepted:** 31/12/2022

**Abstract** – Artificial intelligence (AI) has become an increasingly important tool in the field of cybersecurity, with many organizations using AI-powered systems to defend against cyber threats. In this research paper, we will explore the ways in which AI is being used by enterprises to improve cybersecurity, as well as the potential challenges and limitations of AI in this context.

***Keywords****: artificial intelligence, AI in cybersecurity, cloud computing, cyber-attacks, cybersecurity, enterprises, phishing.*

## 1. Introduction

Artificial Intelligence (AI) has become an increasingly important tool in the field of cybersecurity, with many organizations using AI-powered systems to defend against cyber threats. One of the main ways enterprises uses AI is being used in cybersecurity is to help identify potential security vulnerabilities in networks and systems. AI-powered systems can analyze large amounts of data and use machine learning algorithms to detect patterns that may indicate a security threat. For example, an AI system may be able to detect unusual network activity that could indicate a malware infection or identify a potential vulnerability in a system that could be exploited by an attacker. By identifying these potential security risks, organizations can take corrective action to prevent an attack from occurring.

Another way in which AI is being used in cybersecurity is to automate many of the manual tasks that security analysts currently perform. For example, AI can be used to identify and block malicious websites or emails, or to flag suspicious activity on a network. This can help security teams to be more efficient and effective in their work and allow them to focus on more complex tasks.

AI can also be used to predict and prevent future security threats. By analyzing historical data, AI-powered systems can identify trends and patterns that could indicate a potential attack. This can help organizations to stay one step ahead of cybercriminals and take proactive measures to prevent attacks from occurring.

## 1. What are different types of cyber threats?

There are many different types of cyber threats, and the specific threats that an organization or individual may face can vary depending on several factors. Some common types of cyber threats include

### 1.1 Phishing

Phishing is a type of cyber-attack where the attacker attempts to trick individuals into giving away sensitive information, such as passwords or financial information. This is typically done by sending fake emails or messages that appear to be from a legitimate organization or person. The emails often include a link or attachment that, when clicked, will download malware onto the victim's computer. Phishing attacks can also be carried out through social media, instant messaging, or by phone. The goal of a phishing attack is to obtain sensitive information that can be used for financial gain or to gain unauthorized access to an organization's network or systems.

### 1.2 Malware

A malware attack is a type of cyber-attack where the attacker uses malicious software (known as malware) to damage or disable computer systems. Malware is typically designed to cause harm to computer systems, such as by deleting files, stealing sensitive information, or disrupting the normal operation of a system. There are many different types of malwares, including viruses, worms, and ransomware.

### 1.3 Denial of Service (DoS) Attacks

A denial of service (DoS) attack is a type of cyber-attack where the attacker attempts to make a network or system

(srajasekaran.pm@gmail.com)

unavailable to users by overwhelming it with traffic. This is typically done by sending many requests to the targeted network or system, causing it to become overwhelmed and unable to handle legitimate requests. As a result, users of the network or system may be unable to access it, or the performance of the network or system may be severely degraded. DoS attacks can be carried out by a single attacker or by a group of attackers working together and can cause significant disruption to an organization's operations.

### 1.4 SQL Injection Attacks

An SQL injection attack is a type of cyber-attack where the attacker injects malicious code into a website's database, allowing them to gain access to sensitive information. This is typically done by exploiting vulnerabilities in the website's code, such as by providing input that is not properly validated or sanitized. Once the attacker has gained access to the database, they can steal sensitive information, such as user passwords or financial data, or modify the data in the database. SQL injection attacks can be particularly damaging, as they can allow the attacker to gain access to large amounts of sensitive information and can be difficult to detect.

### 1.5 Man-in-the-Middle Attacks

A man-in-the-middle attack is a type of cyber-attack where the attacker intercepts communication between two parties and alters or steals the information being exchanged. This is typically done by positioning themselves between the two parties and impersonating one or both, allowing the attacker to gain access to sensitive information. Man-in-the-middle attacks can be carried out in several ways, such as by using a fake wireless access point to intercept communications, or by redirecting traffic through a compromised server. These attacks can be difficult to detect, as the communication between the two parties may appear normal to both.

### 1.6 Password Cracking

Password cracking is the process of guessing or using specialized software to determine a user's password. This is typically done by using a dictionary of common words or phrases, or by using a list of previously leaked passwords. Password cracking can also involve using algorithms to generate and test potential passwords, or by attempting to guess the password based on information about the user, such as their name or date of birth. Password cracking is a common tactic used by cybercriminals to gain unauthorized access to accounts or systems. It is important for individuals and organizations to use strong, unique passwords to prevent their accounts from being compromised in this way.

## 2. Ai In Prevention Of Cybercrime Threats

There are several ways AI can help improve and deter cyber threats

### 2.1 Phishing Controls

AI can be used to help prevent phishing attacks by identifying and blocking suspicious emails or messages. AI-powered systems can analyze large amounts of data and use machine learning algorithms to identify patterns that may indicate a phishing attack. For example, an AI system may be able to identify common characteristics of phishing emails, such as the use of urgent language or the inclusion of a malicious link. The system can then automatically block these emails or flag them for further review by security analysts.

Additionally, AI can be used to educate individuals about how to identify and avoid phishing attacks. For example, an AI system could be trained on a large dataset of phishing emails and legitimate emails, and then used to generate simulated phishing attacks that users can practice identifying and avoiding. This can help individuals to develop a better understanding of the tactics used by phishers and to be more cautious when interacting with unfamiliar emails or messages.

Overall, the use of AI in phishing prevention can help organizations to be more effective in identifying and blocking phishing attacks, and to educate their employees about how to avoid falling victim to these attacks.

### 2.2 DNS Data Security

AI can be used to help improve the security of Domain Name System (DNS) data by automatically detecting and blocking suspicious DNS activity. DNS is the system that is used to convert human-readable domain names (such as www.example.com) into the numerical IP addresses that are used by computers to communicate with each other. DNS data can be a valuable target for attackers, as it can be used to gain access to sensitive information or to disrupt the normal operation of a network.

AI-powered systems can monitor DNS traffic in real-time and use machine learning algorithms to identify patterns that may indicate a security threat. For example, an AI system may be able to detect DNS requests that are part of a distributed denial of service (DDoS) attack or identify DNS requests that are being used to exfiltrate sensitive data. The system can then automatically block these requests and alert security analysts to take further action.

Additionally, AI can be used to automate many of the manual tasks that are currently performed by DNS administrators, such as identifying and blocking malicious domain names or tracking the flow of DNS traffic across a network. This can help DNS administrators to be more efficient and effective in their work, and to quickly respond to any security incidents that may arise. Overall, the use of AI in DNS data security can help organizations to better protect their networks and systems, and to identify and respond to potential security threats in real-time.

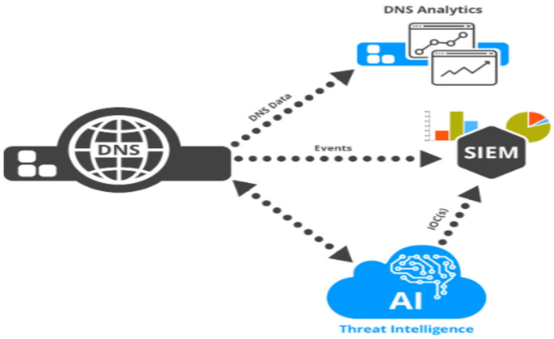

**Fig 1:** AI Powered Secure DNS Service

### 2.3 Authenticity Protection

AI in authenticity protection in cyber security refers to the use of artificial intelligence to help protect against cyber threats and ensure the authenticity of online information. This could include using AI to detect and block malicious content, such as phishing emails or malware, and to verify the identity of users to prevent unauthorized access to sensitive information. AI can also be used in cyber security to help protect the integrity of online data, such as by detecting and preventing the unauthorized alteration of documents or other important information. Overall, the use of AI in authenticity protection in cyber security can help to improve the security of online systems and protect against a wide range of cyber threats.

AI-powered authentication systems can use machine learning algorithms to analyze a wide range of data, such as user behavior or biometric information, to accurately verify the identity of a user or device. For example, an AI system could be trained on data from a user's past login attempts, such as the time of day they typically log in or the locations they typically log in from. The system could then use this data to accurately verify the user's identity in real-time, without requiring them to remember a password or use a security token.

Additionally, AI can be used to automate many of the manual tasks that are currently performed by authentication administrators, such as enrolling users in authentication systems or managing authentication policies. This can help to improve the efficiency and effectiveness of authentication processes and allow administrators to focus on more complex tasks.

## 3. Challenges In Infusing Ai In Cybersecurity

There are several challenges in infusing AI in cybersecurity, including

3.1 The complexity of the cyber threat landscape: The cyber threat landscape is constantly evolving, and it can be difficult for even the most advanced AI systems to keep up with the latest threats.

3.2 The risk of false positives: AI-powered systems are not perfect and can sometimes produce false positives that could lead to unnecessary alarm or disruption.

3.3 The need for high-quality data: AI systems rely on large amounts of high-quality data to function effectively. In the context of cybersecurity, this data can be difficult to obtain, and may not always be accurate or up to date.

3.4 The potential for bias: AI systems can sometimes be biased, either due to the data they are trained on, or the algorithms used to develop them. This can lead to inaccurate or unfair results, which could have negative consequences in the context of cybersecurity.

3.5 Ethical concerns: The use of AI in cybersecurity raises several ethical concerns, such as the potential for AI systems to make decisions that could have negative consequences for individuals or organizations.

Overall, infusing AI in cybersecurity requires careful consideration of these challenges to ensure that AI is used effectively and ethically.

## 4. Ai, Cybersecurity and Geopolitics

The relationship between AI, cyberattacks, and geopolitics is complex and is likely to continue to evolve as AI technology advances. On the one hand, AI can be used to improve the capabilities of cyberattacks, making them more sophisticated and difficult to defend against. For example, AI can be used to automate the process of launching cyberattacks, enabling attackers to target multiple systems simultaneously and making it more difficult for defenders to respond. Additionally, AI can be used to improve the effectiveness of cyberattacks, such as by enabling attackers to target specific vulnerabilities more accurately or to adapt to changing defensive measures.

On the other hand, AI can also be used to improve the ability of organizations and governments to defend against cyberattacks and protect against geopolitical threats. For example, AI can be used to automate the process of identifying and responding to potential cyber threats, enabling organizations to defend against attacks more quickly and effectively. Additionally, AI can be used to improve the security of critical infrastructure and other key assets, making it more difficult for attackers to successfully target them.

There are a few steps that organizations and governments can take to help mitigate the risks and protect against the potential impacts of this relationship. One of the key steps is to invest in the development and deployment of AI-powered cybersecurity technologies. This can include using AI to automate the process of detecting and responding to potential cyber threats, as well as using AI to improve the security of critical infrastructure and other key assets. By investing in AI-powered cybersecurity technologies, organizations and governments can help to improve their ability to defend against cyberattacks and protect against geopolitical threats.

Another important step is to establish effective international cooperation and coordination mechanisms to address the challenges posed by AI, cyberattacks, and geopolitics. This can include initiatives such as developing international norms and standards for the use of AI in cyber security, as well as establishing mechanisms for sharing information and coordinating responses to cyber threats. By working together, organizations and governments can help to ensure that the global community is better prepared to address the challenges posed by AI, cyberattacks, and geopolitics.

Overall, solving the challenges posed by AI, cyberattacks, and geopolitics will require a combination of technological innovation, international cooperation, and ongoing research and development. By taking a proactive and collaborative approach, organizations and governments can help to mitigate the risks and protect against the potential impacts of this complex and evolving relationship.

## 5. The Future

The future of AI in cyberattacks is likely to be characterized by an ongoing arms race between attackers and defenders. As AI technology continues to advance, attackers are likely to increasingly use AI to launch more sophisticated and automated attacks. At the same time, however, defenders are also likely to increasingly use AI to improve their ability to detect and respond to such attacks. As a result, it is likely that the use of AI in cyberattacks will continue to evolve and become more sophisticated over time, with both attackers and defenders using AI to gain an advantage in the ongoing battle for cyber security. In the long run, it is possible that the use of AI in cyberattacks could lead to the development of new types of attacks that are difficult to defend against, as well as new defensive technologies that are specifically designed to counter such attacks.

## 6. Conclusion

AI has the potential to play a significant role in improving cybersecurity by helping organizations to identify potential security threats, automate routine tasks, and predict and prevent future attacks. However, there are also challenges and limitations that need to be considered when using AI in this context. As the use of AI in cybersecurity continues to evolve, it will be important for organizations to carefully balance the benefits and risks of using AI in this context. Artificial intelligence offers many interesting possibilities for protecting networks against cyberattacks, not only for businesses but also for common users of anything digital today.

## References

Khisamova ZI, Begishev IR, Sidorenko EL. Artificial intelligence and problems of ensuring cyber security. International Journal of Cyber Criminology. 2019 Jul 1;13[2]:564–77.

M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi," A primer on cybersecurity," International Journal of Advances in Scientific Research and Engineering, vol. 3, no. 8, Sept. 2017, pp. 71-74.

Guan Z, Li J, Wu L, Zhang Y, Wu J, Du X. Achieving Efficient and Secure Data Acquisition for Cloud-Supported Internet of Things in Smar t Gr id. IEEE Internet of Things Journal. 2017 Dec 1;4[6]:1934–44. https://doi.org/10.1109/jiot.2017.2690522

Dick, S. (2019). Artificial Intelligence. Harvard Data Science Review, 1(1). https://doi.org/10.1162/99608f92.92fe150c

Shamiulla AM. Role of artificial intelligence in cybersecurity. International Journal of Innovative Technology and Exploring Engineering. 2019 Nov 1;9[1]:4628–30. https://doi.org/10.35940/ijitee.a6115.119119

## Disclaimer

This disclaimer informs readers that the views, thoughts, and opinions expressed in this paper belong solely to the authors, and not necessarily to the author's employer, institution or other groups or individuals.

**SureshBabu Rajasekaran** is an experienced product leader with over sixteen years of industry experience and is currently the Group Product Manager at NVIDIA. In his current role, he is focused on helping enterprises to adopt, accelerate and scale AI solutions in their businesses. Suresh worked at companies like Samsung, Adobe, and Autodesk before joining NVIDIA. Suresh is passionate about Artificial Intelligence and its profound impact on Humans. Suresh holds a Masters in Software Engineering from Carnegie Mellon University and an MBA from The University of Chicago Booth school of Business. He currently lives in the San Francisco Bay Area with his wife and two kids.