EasyChair Preprint

№ 11447

A Narrative Overview of Artificial Intelligence Techniques in Cyber Security

Fatima Tahir and Muskan Khan

December 4, 2023

A Narrative Overview of Artificial Intelligence Techniques in Cyber security

Fatima Tahir, Muskan Khan

Abstract:

AI (Artificial Intelligence) plays a significant role in cyber security by enhancing the ability to detect, prevent, and respond to various cyber threats. It brings advanced capabilities to the field that can help organizations stay ahead of rapidly evolving cyber threats

Through this article, we shall study the role of artificial intelligence in the field of cybersecurity. Artificial intelligence (AI) has the potential to significantly aid in cybersecurity efforts by improving threat detection, reducing response times, and increasing the accuracy of security measures.

Keywords: AI, cybersecurity, fishing game, threat detection, hooking.

I. Introduction:

Cybersecurity can be thought of as a fishing game, where the objective is to catch and prevent malicious activity on computer systems and networks. Just like in a fishing game, there are different types of fish (or threats) that require different techniques and tools to catch.

Here are some ways that cybersecurity can be likened to a fishing game[1]:

- Baiting: In a fishing game, different types of bait are used to catch different types of fish. Similarly, cybercriminals use various types of bait such as phishing emails or fake websites to trick users into clicking on links or entering sensitive information.
- Hooking: Once a fish takes the bait, the hook is set. Similarly, once a user falls for a phishing scam or downloads a malicious attachment, the attacker has a foothold in the system and can begin their attack.
- Reeling in: Once a fish is hooked, the goal is to reel it in quickly and safely. In cybersecurity, once an attack is detected, the goal is to contain it and prevent further damage.
- Luring: In a fishing game, anglers may use lures to mimic the movement of a particular type of fish and attract it to the bait. Similarly, attackers may use social engineering techniques to manipulate users into divulging sensitive information or downloading malware.
- Casting a wide net: In a fishing game, anglers may cast a wide net to increase their chances of catching a fish. Similarly, attackers may use mass spam email campaigns or other automated tools to target a large number of potential victims.

Overall, just like in a fishing game, successful cybersecurity requires a combination of the right tools, techniques, and strategies to catch and prevent threats[1].

Cybersecurity and artificial intelligence (AI) are becoming increasingly interconnected as AI technology is being developed to improve cybersecurity measures[2-4]. AI has the potential to enhance cybersecurity by detecting, preventing, and responding to cyber threats more effectively than traditional methods [5].

Cybersecurity and artificial intelligence:

Here are some ways AI can improve cybersecurity:

- Threat detection: AI can be trained to identify patterns and anomalies in network traffic, which can help detect potential cyber attacks. AI-powered threat detection systems can analyze vast amounts of data quickly and accurately, allowing cybersecurity professionals to respond to threats in real-time [6].
- Automated response: AI can also be used to automate response actions to known threats, such as quarantining an infected device or blocking malicious traffic. This can reduce the response time and limit the damage caused by a cyber attack[7, 8].
- Behavioral analysis: AI can be used to analyze user behavior and identify suspicious activity, such as unusual login times or attempts to access sensitive data. This can help detect insider threats or compromised user accounts.
- Vulnerability assessment: AI can be used to scan networks and identify vulnerabilities that could be exploited by attackers. This can help prioritize security patches and reduce the risk of a successful cyber attack.
- Predictive analytics: AI can be used to analyze historical data to predict future threats and help organizations proactively defend against them.

However, it is important to note that AI technology is not a silver bullet for cybersecurity. It is still necessary to have a multi-layered defense strategy that includes human expertise, as well as traditional security measures such as firewalls, anti-virus software, and access control. Additionally, AI-powered security systems are not immune to cyber attacks themselves and require continuous monitoring and updating to stay effective.

Here are some reasons why we should use AI for cybersecurity:

Increased speed and efficiency: AI can quickly and accurately analyze vast amounts of data to identify threats, reducing the response time to potential attacks and increasing the efficiency of security measures.

Improved accuracy: AI can help reduce the number of false positives and false negatives in threat detection, improving the accuracy of security measures.

Constant monitoring: AI can work 24/7 to monitor networks and systems for potential threats, providing continuous protection against cyber attacks.

Early detection: AI can help detect and prevent attacks before they cause damage by identifying and responding to potential threats in real-time.

Proactive defense: AI can help organizations take proactive measures to defend against potential attacks by analyzing historical data and predicting future threats.

II. Conclusion:

After all the study, the question of using artificial intelligence in cybersecurity is answered through research. Yes, the use of artificial intelligence (AI) for cybersecurity is becoming increasingly necessary as cyber threats continue to become more sophisticated and complex. AI technology has the potential to significantly enhance cybersecurity by improving threat detection, reducing response times, and increasing the accuracy of security measures.

References:

[1] A. Lakhani, "AI Revolutionizing Cyber security unlocking the Future of Digital Protection," 2023, doi: https://osf.io/cvqx3/.

[2] A. Lakhani, "ChatGPT and SEC Rule Future proof your Chats and comply with SEC Rule," 2023, doi: https://osf.io/h7z43/.

[3] A. Lakhani, "Enhancing Customer Service with ChatGPT Transforming the Way Businesses Interact with Customers," 2023, doi: https://osf.io/7hf4c/.

[4] A. Lakhani, "The Ultimate Guide to Cybersecurity," 2023, doi: 10.31219/osf.io/nupye.

[5] D. Ghelani and T. K. Hua, "Conceptual Framework of Web 3.0 and Impact on Marketing, Artificial Intelligence, and Blockchain."

[6] D. Ghelani, T. K. Hua, and S. K. R. Koduru, "Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking," *Authorea Preprints,* 2022.

[7] N. Mazher, M. Alhadaad, and O. Shagdar, "A Brief Summary of Cybersecurity attacks in V2X Communication," 2022.

[8] J. Bosch, H. H. Olsson, and I. Crnkovic, "It takes three to tango: Requirement, outcome/data, and AI driven development," in *SiBW*, 2018, pp. 177-192.