Aykhan Pashayev

Y. Acuna

ENC 1102

Date: 4/17/2024

Link for the website: *https://new.express.adobe.com/webpage/X52jmpWO0sD8R*

Artificial Intelligence (AI)'s role in Cybersecurity

Introduction

In an era where the digital landscape is increasing constantly, the need for strong cybersecurity measures has become critical. "Cybersecurity, the shield that protects our digital areas from threatening attacks, includes a wide range of techniques, technologies, and practices designed to secure sensitive information, vital infrastructure, and digital assets from cyber threats". At its foundation, cybersecurity is the first line of protection against a wide range of cyber threats, such as malware, ransomware, phishing attacks, data breaches, and so on. The primary goal is to detect, prevent, and minimize these threats in order to protect the confidentiality, integrity, and availability of data and systems.

At the same time, artificial intelligence (AI) is growing as a transformational force across multiple fields, changing companies and reshaping how we address complicated challenges. AI, a discipline of computer science that focuses on developing intelligent machines capable of replicating human-like behavior and decision-making processes, has made extraordinary progress in recent years.

The relationship between AI and cybersecurity is absolutely nothing short of revolutionary. AI technologies such as machine learning, natural language processing, and neural networks provide cybersecurity experts with new tools and skills for successfully battling changing cyber threats. According to expert with AI Arroyo-Figueroa these AI-powered solutions are flexible and adaptable enough to scan massive datasets, spot trends, detect anomalies and predict future cyber threats in real time. However, while AI has tremendous potential for improving cybersecurity defenses, it also represents new problems and hazards. The same AI algorithms that improve threat detection and response can be utilized by hackers to create more complex and difficult attack methods. Furthermore, AI-powered attacks can self-adapt and develop, creating a huge danger to the existing cyber world.

In this article, we will look at both the benefits and disadvantages of AI in cybersecurity, including its revolutionary potential, rising dangers, and the changing environment of digital defense. From active threat hunting to AI-driven fraud techniques, we'll look at the cutting-edge innovations that are transforming the cybersecurity landscape and impacting the future of digital defense.

Potential applications of AI in Cybersecurity

Artificial intelligence (AI) is of tremendous interest to cybersecurity professionals. According to Italian AI expert Bergadano, AI has potential uses in cybersecurity due to two key characteristics:

1. Detecting new and challenging attacks is difficult for traditional security systems since they only know about previous attempts. However, with AI, we can detect hazards by observing how programs and networks act. Smart security systems learn from what is typical, allowing them to detect anything unusual that could represent a threat.

2. Every day, a large volume of data flows through networks, making it difficult to detect attacks quickly and accurately. However, AI can assist by developing automated security systems that scan through all of that data, detect threats, and take appropriate action to fight against them. With AI, we can detect hazards automatically and respond in real time, allowing us to identify and deal with them more quickly and effectively.

According to Arroyo-Figueroa let's explore how AI is being used by Cyber experts?

Detection of malware. Detecting malware often depends on traditional methods that hunt for certain signs. However, there are two problems: they cannot detect new malware, and they suffer when malware attempts to avoid detection through changing its look. AI addresses this by learning from how malware evolves over time. It uses clever algorithms to analyze various malware assets and behaviors, allowing it to better identify and alert potential dangers.

Intrusion detection. Intrusion detection prevents cyber dangers by detecting and responding to unwanted access attempts. An Intrusion Detection and Prevention System (IDPS) acts as a network security guard, alerting you to any unusual or possibly harmful activity. AI algorithms are ideal for developing these systems because they can immediately learn and adapt to various threats, making them adaptable and capable of responding quickly to keep your network safe.

Phishing detection. Phishing occurs when criminals send fake messages appearing to be from reputable organizations in order to confuse clients into giving sensitive information such as passwords or credit card numbers. AI can assist prevent phishing attempts by identifying them in the same way that a detective would.

Advanced Persistent Threat (APT). An Advanced Persistent Threat (APT) is a secretly attack tactic in which able hackers collaborate to steal sensitive data while remaining hidden on

infected devices for a long amount of time. AI can assist detect and prevent APT assaults by monitoring for unusual activities. AI can decrease the damage caused by APT by detecting intrusions early on and responding quickly.

Automated risk analysis and impact assessment. Automated risk analysis and impact assessments are like super-intelligent assistants for the risk management staff. They analyze a variety of data, both within and outside the firm, to rapidly figure out how unsafe something is and what consequences it may have. With AI handling the hard pulling risk scoring becomes faster, allowing the team to manage risks more effectively.

Predictive intelligence. Predictive intelligence is similar to having a crystal ball for cybersecurity. It's all about using intelligent technologies to predict possible attacks before they occur. By preparing for the form, strength, and target of future attacks, intrusion prediction technology helps maintain defenses robust and ready to face new attacks.

Data leakage prevention. Data leakage prevention is all about keeping sensitive information from falling into the wrong hands. It operates by monitoring how data is accessed, transferred, and used, and it can detect hidden risks such as APT assaults. Using artificial intelligence, it can detect suspicious activity and prevent data leaks before they do harm.

AI-powered backup. AI-powered backup. AI-powered backup solutions are beginning to back up crucial data and software components based on objectives and needs, resulting in efficient backup. AI approaches are used to schedule backups automatically and accurately.

The growing danger

Nevertheless, while AI has been applied to improve cybersecurity defenses, it has also introduced new difficulties and risks. AI may be used by hackers to develop more complicated

and challenging cyberattacks. Cyberattacks are pervasive and are often regarded as one of the most tactically significant risks confronting the world today. Cybercrimes can engender disastrous financial losses and affect individuals and organizations as well.

“It is estimated that a data breach costs the United States around 8.19 million Dollars and 3.9 million Dollars on average, and the annual effect on the global economy from cyberattack is approximately 400 billion Dollars” (Kaloudi, Nektaria, and Jingyue Li, 2021).

A Cyberattack is the intentional exploitation of computer systems, networks, and businesses. With increasingly sophisticated cybersecurity attacks, cybersecurity specialists are becoming incapable of addressing what has become the most significant threat climate ever before.

Today’s current wave of attacks outwits and outpaces humans and even includes Artificial Intelligence. Cybercriminals will be able to direct targeted attacks at unprecedented speed and scale while avoiding traditional, rule-based detection measures thanks to what’s known as “offensive AI”. The new generation of cyber threats will be smarter and capable of acting independently with the help of AI. Future cyberattack methods will be able to be aware of their surroundings and make informed decisions based on the target environment. The consequences of these emerging AI-driven attack techniques could be life-threatening and highly destructive.

AI as tool for cyber criminals

Automated Payload Generation/Phishing. Bad guys can use machine learning to generate more dangerous phishing emails." These emails may pass through cybersecurity measures undetected.

AI-Driven DDoS Attack. The use of AI in DDoS attacks brings in a new age in which humans are no longer needed. These assaults are entirely automated, with robots attacking apps and complex

cybersecurity security measures. They may change strategies on their own, switching to alternative approaches if one fails, all without assistance from humans.

Next-generation password brute-force attack. The next generation of password brute-force attacks uses AI that continues to grow and adapt. They look at existing passwords to generate new ones that are more likely to work. These assaults get deeper with each try as they learn patterns from previous password use.

Social Bots. Machine learning is helping improve social bots. Attackers can build clever botnets made of smart bots that can operate independently. These bots may examine their environment, determine what to do, and execute out attacks without human assistance.

DeepPhish. DeepPhish is an AI algorithm that generates new phishing website connections. It learns from successful previous attacks to make its connections seem more credible. The goal is to fool humans more successfully while avoiding detection by AI systems. In the past, attackers used random connections, which were easily detected. DeepPhish is smarter and more difficult to detect.

DeepHack. DeepHack is an AI-powered hacking tool that anybody may use. It learns itself how to break into web application databases without requiring any prior knowledge of the technology. It uses fuzzing logic to automate hacking work. Despite previous approaches, which need attackers to provide exact directions, DeepHack develops to hack on its own.

The battle against AI.

The AI danger keeps rising, but cyber specialists are always ready to battle. The fight against AI-powered dangers requires a dedication to constant development and adaptation. Cybersecurity experts must keep current on the newest developments in AI technology and cyber-attack

methods. Understanding harmful attackers' skills and tactics allows defenders to actively change their security strategies, keeping them one step ahead. The fight against AI-powered cyber-attacks is too complicated for every organization to handle alone. So, collaboration is very crucial. By taking all of these actions, cyber professionals may successfully limit the threats presented by AI-driven harmful operations while also protecting the digital environment for future generations.

Conclusion

In today's fast-paced world of technology, where artificial intelligence and cybersecurity compete, effective defenses are more important than ever. While AI provides excellent threat detection capabilities for defenders, it also provides new attack pathways for criminals. In this changing scenario, cyber specialists are leading the effort to safeguard our digital world. We can defend ourselves against AI-driven attacks by remaining alert, developing together, and staying strong. Our efforts not only protect this moment, but also create a solid barrier for the future of our digital world.

Reflection

The role of artificial intelligence (AI) in cybersecurity was the focus of my research. Although I am studying cybersecurity and hope to work in the sector successfully in the future, artificial intelligence has always been part of my curiosity because it is developing rapidly in almost every field. Though I knew AI had a significant influence on many industries, I had never considered how it would affect cybersecurity. It took me a long time to read all of the really excellent sources I found, but it was enjoyable since I learned a lot of new stuff. People who are interested in AI, cybersecurity, and technology and who analyze the future of those fields are my target

audience. However, it seemed to me that I should use as straightforward language as possible for easier understanding while I was reading and saw new terminology. Therefore, I'm hoping that someone who reads the article and isn't too familiar with the technology industry will be able to understand it. I wanted to express to the audience the feeling of the cyber world, artificial intelligence, and hacking, therefore at the opening of the online page, you can see a person whose face is hidden under a black hoodie and a lot of codes. In order to make sure that even those who are not familiar with the IT industry can understand what is being discussed in this article, I wanted to begin with some basic definitions of AI, cybersecurity, and how the two relate to one another. Then I addressed both the benefits and disadvantages of artificial intelligence. After that, I highlighted how cyber professionals may fight with offensive AI and ended with conclusion. I believe this format will be straightforward and easy to understand for the audience. The images I chose show both cybersecurity and artificial intelligence, and each image matches with the subtitle. For example, in *the growing danger part*, you may witness a scary robot coding on a computer or a robot and human facing off in *the battle against AI* part. I used a quote regarding the costs of data breaches in the United States to highlight to the audience the value of digital security. Finally, I had a great time learning new things. I attempted to clarify complicated words in simple terms. By highlighting both the benefits and challenges of AI in cybersecurity, I hope to inspire proactive actions within the industry and ensure a safe digital future.

References:

1. Arroyo-Figueroa, Gustavo. “Artificial Intelligence the Strategic Key of Cybersecurity.” International Journal of Combinatorial Optimization Problems & Informatics, vol. 14, no. 3, Sept. 2023, pp. 16–23. EBSCOhost, https://doi.org/10.61467/2007.1558.2023.v14i3.372.
2. Bergadano, Francesco, and Giorgio Giacinto. “Special Issue ‘AI for Cybersecurity: Robust Models for Authentication, Threat and Anomaly Detection.’” Algorithms, vol. 16, no. 7, July 2023, p. 327. EBSCOhost, https://doi.org/10.3390/a16070327.
3. Guembe, Blessing, et al. “The Emerging Threat of Ai-Driven Cyber Attacks: A Review.” Applied Artificial Intelligence, vol. 36, no. 1, Dec. 2022, pp. 1–34. EBSCOhost, https://doi.org/10.1080/08839514.2022.2037254.
4. Kaloudi, Nektaria, and Jingyue Li. “The AI-Based Cyber Threat Landscape: A Survey.” ACM Computing Surveys, vol. 53, no. 1, Jan. 2021, pp. 1–34. EBSCOhost, https://doi.org/10.1145/3372823.
5. Kaur, Ramanpreet, et al. “Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions.” Information Fusion, vol. 97, Sept. 2023, p. N.PAG. EBSCOhost, https://doi.org/10.1016/j.inffus.2023.101804.
6. Mazurczyk, Wojciech, et al. “Disinformation 2.0 in the Age of AI: A Cybersecurity Perspective.” Communications of the ACM, vol. 67, no. 3, Mar. 2024, pp. 36–39. EBSCOhost, https://doi.org/10.1145/3624721.