precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 20

APRIL 2023

Today we are going to be discussing Artificial Intelligence and how it is implemented in Cybersecurity.

Dr. Ronald Walcott
Managing Director

As time goes on and technology develops more and more, many different industries have been utilizing a certain technology that exponentially increased efficiency. What is this technology? It is known as Artificial Intelligence or machine learning. AI is being implemented in many different industries and is even available to individuals for personal usage.

WHAT IS ARTIFICIAL INTELLIGENCE?

While there are many different definitions of artificial intelligence, for the purpose of this article, we will define AI as, "the science and engineering of making intelligent machines, especially intelligent computer programs." There are typically two types of artificial intelligence. The first is weak AI, also known as Narrow AI. This refers to AI that's trained and focused to perform specific tasks. This type of AI is what surrounds us every day. This type of AI is not actually weak but in fact enables robust applications and technology such as Apple's Siri and Amazon's Alexa. Secondly, there is Strong AI. This refers to a theoretical form of intelligence where a machine would have intelligence mirroring that of a human, meaning the machine would have some self-awareness, and have the ability to solve problems, learn and plan for the future. The closest and most recent example of this type of AI developed is with the Sophia robot.

Deep learning Vs Machine Learning

These two terms have been used interchangeably, but there are some nuances between the two. Deep learning and machine learning are both artificial intelligence, however they are sub-fields or categories of AI, and deep learning is actually a sub-field of machine learning. Deep learning differs from machine learning in that deep learning automates much of the feature extraction process, thereby eliminating the need for manual human intervention and allows for the use of larger data sets. On the other hand, machine learning depends more on human intervention for learning. The technology learns the behavior and patterns of human experts to determine the behavior of the AI technology. In the industry of Cybersecurity, we rely on AI that uses machine learning technology to learn from security professionals to determine what are threats or what is allowed.

HERE ARE SOME COMMON APPLICATIONS OF ARTIFICIAL INTELLIGENCE

Speech Recognition: Also known as Automatic Speech Recognition, this AI has the capability to process human speech into text format. For ex-

In this Issue:

ample, Apple's Siri, Samsung's Bixby, etc.

Computer Vision: This type of AI technology enables computer systems to derive meaningful information from digital images, videos, etc. and based on those inputs, the AI can take action. Powered by convolutional neural networks, computer vision has applications within photo tagging in social media, radiology imaging in healthcare, and self-driving cars within the automotive industry.

HERE IS AN EXAMPLE OF HOW AI IS IMPLEMENTED IN CYBERSECURITY.

IBM's QRadar: allows for organizations to enhance the capabilities of their security information and event management solutions. It gives the organization greater insight and gives you a more proactive role in your organization's information security. Qradar utilizes machine learning so that cyber security teams can focus their efforts on critical security concerns while analysts oversees and monitors SOC threats. Qradar gives deep insights into network traffic and or potential breaches and attacks. It reconstructs data in a security incident for IT teams to have greater visibility and simplifies data.

Cyber AI: This type of AI enables companies to respond faster than attackers, anticipate moves that attackers make and react to attacking strategies in advance. This technology has the ability to adaptively learn and detect novel patterns can accelerate detection, containment, and response, easing the burden on SOC analysts and allowing them to be more proactive.

PROS OF AI IN CYBERSECURITY

Faster threat detection and Response

By leveraging AI, you can better understand your networks and identify potential threats faster than ever. AI solutions can sift through vast amounts of data to identify irregular behavior and quickly detect malicious activity, such as a new zero-day attack.

Greater Scalability and Cost Efficiency

AI solutions are easily scalable thereby opening the possibility of purchasing increased protection without much hardware or an increase in personal costs.

Improved Accuracy and Efficiency

AI based cyber security solutions provide exponentially greater accuracy and efficiency that traditional security solutions. AI can scan devices and network patterns for potential vulnerabilities in a fraction of the time that it would take a human.

CONS OF AI IN CYBERSECURITY

Biased Decision-making

AI systems can make biased decisions on data sets if it lacks objectivity. These biases can lead to discrimination if against individuals or groups in an organization.

Lack of Explainability or Transparency

AI solutions may be difficult to interpret which would make it hard for personnel to understand why certain decisions were made.

Potential Misuse or Abuse

Cybersecurity professionals are not the only ones utilizing AI solutions. Cyber criminals are also using AI to gain access to sensitive information.

Frequently Asked Questions:

DOES AI MEAN THAT THE SOFTWARE/TECHNOLOGY CAN OPERATE ON ITS OWN?

AI technology has some level of independence. It can make some automated decisions which makes it seem like it operates completely on its own.

CAN AI ALSO AID CYBER CRIMINALS?

Cyber criminals do also use AI technology to carry out malicious activity. They use AI to create new sophisticated attacks, making it extremely difficult for reputation engines to keep up.

HAS AI BECOME NECESSARY IN DEFENDING AGAINST CYBERCRIMES AND ATTACKS?

The rate at which attacks happen today, and the speed at which they are executed are too fast for humans to keep up. Therefore, AI technology help identify, defend and recover from malicious activity.

Upcoming Events

ISMG ENGAGE
May 11, 2023
London

CYBERSECURITY SUMMIT: NORTH AMERICA-WEST
May 23, 2023

ISMG ENGAGE
June 11, 2023
Chicago

Headline News

How Security Vendors Can Strengthen Their Security Posture

Cybersecurity involves not just surviving a cyberattack but ensuring compliance and managing the vast ecosystem of employees, contractors, vendors and other third parties that touch your organization. It's "a full-time task," said Ajay Sabhlok, CIO and chief digital officer at Rubrik.Sabhlok stressed discipline and education as requirements for a secure posture. "At the heart," he said, "are the individuals you hire." Train them well, he said.

As for vendors, Sabhlok said they should emphasize quality over time to market for their products.

In this video interview with Information Security Media Group at RSA Conference 2023, Sabhlok also discusses:

- The recent zero-day attack Rubrik experienced;
- Rubrik's motto: "Don't pay the ransom" and its ransomware recovery warranty;
- How CISOs may be responsible for security strategy while CIOs focus on execution.

Prior to Rubrik, Sabhlok led multiple IT application portfolios at VMware, including marketing, customer support, order management, sales, business intelligence, advanced analytics, master data management and more. Over the past few years, he has been instrumental in leading the IT, applications and infrastructure teams at Rubrik, implementing a number of successful projects. **Source: www.databreachtoday.com**