**AI In Cybersecurity**

Artificial intelligence poses both a blessing and a curse to businesses, customers, and cybercriminals alike.

AI technology is what provides us with speech recognition technology (think Siri), Google’s search engine, and Facebook’s facial recognition software. Some credit card companies are now using AI to help financial institutions prevent billions of dollars in fraud annually.

On one hand, artificial intelligence in cyber security is beneficial because it improves how security experts analyze, study, and understand cybercrime. It enhances the cyber security technologies that companies use to combat cybercriminals and help keep organizations and customers safe. On the other hand, artificial intelligence can be very resource intensive. It may not be practical in all applications. More importantly, it also can serve as a new weapon in the arsenal of cybercriminals who use the technology to hone and improve their cyberattacks.

In addition, AI – based cyber security systems can provide effective security standards and help develop better prevention and recovery strategies.

Alternatively, the use of AI for cyber security helps to create a dynamic, real – time, global authentication framework that changes location or network access privileges.

In fact, more than 90 percent of US and Japan’s cybersecurity professionals expect attackers to use AI for the companies they are working for, according to a study by Webroot.

Enterprise AI initiatives have a wide range of potential vulnerabilities, including malicious corruption or manipulation of training data, implementation and component configuration.

Darktrace’s cybersecurity company claims that its automatic machine learning technology has identified 63, 500 previously unknown threats on more than 5, 000 networks, including zero – day exploits, internal threats and subtle, hidden attacks.

From network and web application security to threat protection and unified and secure access, Fortinet’s cyber security products are used by most Fortune 500 companies.

**Drawbacks and Limitations of Using AI for Cybersecurity**

There are also some limitations that prevent AI from becoming a mainstream security tool:

* Resources—companies need to invest a lot of time and money in resources like computing power, memory, and data to build and maintain AI systems.
* Data sets—AI models are trained with learning data sets. Security teams need to get their hands on many different data sets of malicious codes, malware codes, and anomalies. Some companies just don’t have the resources and time to obtain all of these accurate data sets.
* Hackers also use AI—attackers test and improve their malware to make it resistant to AI-based security tools. Hackers learn from existing AI tools to develop more advanced attacks and attack traditional security systems or even AI-boosted systems.
* Neural fuzzing—fuzzing is the process of testing large amounts of random input data within software to identify its vulnerabilities. Neural fuzzing leverages AI to quickly test large amounts of random inputs. However, fuzzing has also a constructive side. Hackers can learn about the weaknesses of a target system by gathering information with the power of neural networks. Microsoft developed a method to apply this approach to improve their software, resulting in more secure code that is harder to exploit.

**Applications of Artificial Intelligence in Cybersecurity**

* Vulnerability Management: Currently, the security solutions wait for the vulnerabilities in the IT infrastructures and then take action on them, depending on its nature. The approach becomes different from AI and ML-enabled tools. The AI-based systems are proactive in detecting the vulnerabilities. They can analyze the pattern and discover the loose ends that can be the potential vulnerability.

By recognizing the attackers’ pattern, infiltrating methods can be discovered, and it becomes easy to distinguish when and how any vulnerability would make its way to the network or system.

* Improving the Authentication: Most organizations and individuals are still dependent on the traditional method of entering the login id and password for authentication purposes. Let us face it, there are very few people who are serious about creating a unique and strong password. Over that, most people use the same passwords for all or most of their accounts. Such practices can lead organizations or individuals to serious security risks.

However, with modern biometric authentication methods such as face recognition and iris recognition, login authentication has become highly secure and comfortable. The use of AI in biometrics has ensured that cybercriminals cannot hack them.

* Behavioral Analysis: Another great advantage of Artificial Intelligence in cybersecurity is its behavioral analysis ability. AI can develop a pattern by accessing users’ working methods. If any malware is introduced in the system, the working way would be changed, and that’s where the AI would detect the abnormality and report it to the authorities. The abnormalities could be anything like the unusual use of the internet, change in the typing speed, increment in the background activities, and more.
* Controlling Phishing: Phishing is one of the most common cyber-attacks used by hackers to capture the login credentials or introduce the malware into the system. Artificial Intelligence can be of great help in detecting and preventing phishing attacks. AI can detect the most common phishing sources and report them to the system to prepare for the defense against it. AI can easily recognize the difference between a fake and a legitimate website in no time. It can also analyze the phishing pattern according to the specific geographical location.
* Threat Hunting: As already mentioned, the traditional security programs use signature indicators to detect threats. This technique is only effective with the already encountered attacks and becomes useless when reporting the threats that have never appeared. Using the AI, the new threats can be recognized quickly. However, with it, the false-positive cases would also increase. To eliminate the number of false-positives, both the traditional detecting method and the AI behavioral analysis detection must be combinedly used.

**Conclusion:**Artificial intelligence and machine learning can improve security, while at the same time making it easier for cybercriminals to penetrate systems with no human intervention. This can bring significant damage to any company. Getting some kind of protection against cyber criminals is highly recommended if you want to reduce losses and stay in business.