Campus: IIE MSA Ruimsig Campus

Module Name: Principles of Security

Module Code: PRSE

Assignment Type: Ice Task 1

Student Name: Peace Salomy Phiri

Student Number: ST10163788

Introduction

Cyber Security is the practice of protecting electrical systems, servers and important data from malicious attacks. With increase in cyber threats, cyber security has become important. The following are the types of Cyber threats, Cyber Crime, Cyber Attack and Cyber Terrorism. Cybercriminals use different methods to threaten Cyber-Security for instance, the use of Malware. This is a software the cybercriminal creates to disrupt and damage a user’s computer. Malware also has different types including Virus and Trojan (KasperSky, 2019).

Artificial intelligence on the other hand is the process of teaching a machine to make judgments on its own (socialchamp, 2023). Machine learning is a branch of artificial intelligence which focuses on data and algorithms to simulate how people learn and improve its accuracy (IBM, 2023). The two are crucial in a variety of ways. For instance, it is important in Cyber Security. Below are some points to show how important Artificial Intelligence and Machine Learning are important in cyber security.

First and Foremost, Identification of Cyberattacks. AI can be used to identify cyberattacks in advance of any attack that might happen unexpectedly. Hackers present around the world use different methods to hack and launch cyberattacks. So organizations that need high security are completely dependent on AI to provide high security. And so it will be difficult for hackers to access websites or any important information when they use AI for security. Since AI can identify cyber-attacks even before they happen, this makes it a good security provider against attacks carried out by hackers (Prasad and Rohokale, 2019).

Secondly, Securing Authentication. AI provides this layer of security by using tools like facial recognition and fingerprint scanners for secure authentication during login attempts. This helps detect fraudulent login attempts and prevents brute-force attacks and credential stuffing, which can lead to potential security holes in your network (Engati, 2021).

Furthermore, Threat detection. It helps identify vulnerabilities and weaknesses in systems and networks. By continuously monitoring potential threats, organizations can prioritize and address these vulnerabilities quickly, reducing the likelihood of successful attacks and mitigating the associated risks (Dr. Geethamanikanta Jakka, 2022).

Moreover, ML and AI techniques can continuously monitor network traffic, system logs, and user behavior in real time. By analyzing this data, they can quickly identify suspicious activity, such as unusual network traffic, unauthorized access attempts, or unusual user behavior. This allows security teams to react quickly and mitigate potential threats before they cause significant damage.

In-addition, Automated Threat Analysis (Breathing space for human cyber security teams.). AI helps security analysts control a growing number of threats by automatically assessing malware, detecting botnets, and identifying large-scale phishing emails. This frees up human time and bandwidth (Rekha et al., 2020).

More of it, Fraud Detection. ML and AI algorithms can be used to detect fraudulent activity, such as credit card fraud, identity theft, or phishing attacks. By analyzing transaction data, user behavior, and historical patterns, these techniques can identify suspicious activity and flag potentially fraudulent transactions.

To add, Security analysis and threat intelligence (Handling huge volumes of security data). Machine learning and artificial intelligence (ML and AI) can assist in the analysis of huge amounts of security data, including as logs, vulnerability assessments, threat intelligence feeds, and security incident reports. Security experts can discover trends, anticipate potential risks, and create preventative security measures by drawing insightful conclusions from this data (Rekha et al., 2020).

However, Artificial intelligence can prevent cyberattacks. Just identifying the threat is not enough and can't really keep websites away from hackers and cyberattacks. AI can be used to prevent cyberattacks in many ways. Here, the AI ​​has to think about how a hacker might think about hacking the website and then act accordingly. Hackers tend to keep an eye on the website they need to attack and figure out how and how to do it. (Prasad and Rohokale, 2019).

Last but not least, for malware detection, ML has made a big difference with its ability to analyze static or dynamic files or code and determine if they are malicious with great accuracy. Traditional signature-based antivirus engines are not effective against new malware, but ML models can recognize malicious patterns even in files they've never seen before. They are trained on large datasets of known malware, allowing them to generalize and detect new malware variants. This fills a major hole in traditional malware defenses.

To conclude, integrating AI and ML into cybersecurity has changed the way we protect our digital assets. These technologies provide advanced threat detection, enable real-time response, and automate common security tasks. While challenges remain, the benefits of AI and ML in cybersecurity far outweigh the risks. As the cybersecurity landscape continues to evolve, AI and ML will play an increasingly important role in protecting against emerging threats, ensuring the security and integrity of the facility of our digital infrastructure.

REFERENCES

IBM (2023). *What is Machine Learning?* [online] www.ibm.com. Available at: <https://www.ibm.com/topics/machine-learning>.

‌ www.kaspersky.com. (2020). *AI and Machine Learning in Cybersecurity — How They Will Shape the Future*. [online] Available at: <https://www.kaspersky.com/resource-center/definitions/ai-cybersecurity>.

Engati. (n.d.). *8 benefits of using AI in cybersecurity*. [online] Available at: <https://www.engati.com/blog/ai-for-cybersecurity>.

www.socialchamp.io. (n.d.). *What is Artificial Intelligence? | Social Champ*. [online] Available at: <https://www.socialchamp.io/social-media-glossary/artificial-intelligence/?kw=socialchamp&msclkid=d239409c600212954dba2448f4c0fa1d>.

Prasad, R. and Rohokale, V. (2019). Artificial Intelligence and Machine Learning in Cyber Security. *Springer Series in Wireless Technology*, pp.231–247. doi: <https://doi.org/10.1007/978-3-030-31703-4_16>.

IBM (2023). *What is Machine Learning?* [online] www.ibm.com. Available at: <https://www.ibm.com/topics/machine-learning>.

Jakka, D.G., Yathiraju, N. and Ansari, D.M.F. (2022). Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management. *Journal of Positive School Psychology*, [online] 6(3), pp.6156–6165. Available at: <https://journalppw.com/index.php/jpsp/article/view/3522/2300>.

‌

‌

‌

‌

‌

‌