www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 12 Issue 11 November 2023, Page No. 25942-25947
ISSN: 2319-7242 DOI: 10.18535/ijecs/v12i11.4776

AI-Based Cybersecurity Solutions in Threat Detection and Incident Response

Ritama Pal[1], Arpita Chakraborty[2], Anirban Bhar[3], Moumita Ghosh[4]

[1,2] B. Tech student, Department of Information Technology, Narula Institute of Technology, Kolkata, India.
[3,4] Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.

Abstract

This work provides an in-depth analysis of the impact of artificial intelligence (AI) in cybersecurity. With the rise of cybercrime and the increasing sophistication of cyberattacks, organizations are implementing advanced cybersecurity measures, and AI is emerging as a critical tool. The work discusses the benefits of AI in cybersecurity, including enhanced threat detection, reduced false positives, automation, improved response time, and predictive analytics. However, it also highlights the challenges associated with AI in cybersecurity, such as lack of transparency, bias, adversarial attacks, integration, and skill gap. The work concludes that AI is not a panacea for all cybersecurity problems, but it is a critical tool that can help organizations defend against ever-evolving cyber threats. Addressing the challenges associated with AI in cybersecurity requires ongoing monitoring and refinement to ensure that AI-powered cybersecurity solutions remain effective and secure. Finally, the work identifies ethical considerations and regulatory frameworks that organizations must consider when implementing AI in cybersecurity. Overall, this work provides valuable insights into the current state and future of AI in cybersecurity and highlights the importance of a holistic approach to cybersecurity.

Keywords: Artificial Intelligence (AI), Cybersecurity, Cybercrime, Threat detection, Predictive analytics, Adversarial attacks, Holistic approach.

1. Introduction

Cyber security protects records/statistics, property, services, and systems of cost from loss, damage/corruption, compromise, or misuse to a level commensurate with the cost. Controlling system data access became a major issue in the mid to late 1960s when time-sharing systems allowed multiple jobs and users to work simultaneously. One solution was to sort data one level at a time and "sanitize" the device after one stage's jobs were run and before the next stage. Because every level's jobs were done at its own time, this computer security method was called durations processing. This makes using the gadget wasteful, hence green software solutions to the multilevel security problem are sought. Adding features or mechanisms to a laptop is another way to improve security. This phase includes authentication, control access, and inference manipulation. A system's safety can also be improved by subjecting it to strict warranty policies to boost confidence in its performance. Penetration analysis, formal specification and verification, and covert channel evaluation are examples. None of these methods guarantee system stability. The best boost is self-confidence in the device's safety [1].

In the Initial Response, event data is collected as in the preceding section. Data collection is needed to create an effective response technique in the next step. This step usually involves interviews with those reporting the suspected incident and network surveillance logs or IDS evaluations, which may indicate an incident. The response technique involves "thinking about the totality of the occasions" surrounding the incident. These events include the criticality of the affected systems or data, the suspected attacker, and the potential damage. A company's response posture, which determines its computer security response coverage, can also influence its reply approach. In order to reconstruct the computer protection incident, host- or network-based evidence is collected during the investigation. This reconstruction should explain what happened, when, how, and who is responsible. To do this, an inquiry normally involves data collection and analysis. The Resolution portion is used to contain an incident, fix the root cause, and prevent a repeat. To ensure their efficacy, all necessary actions must be followed and monitored. The impacted systems should be adjusted after gathering viable evidence, otherwise the evidence may be lost. After the situation is resolved, protective rules or IR approaches may need to be updated if the reaction revealed a weakness in current practice [2].

Cyber security personnel can better assess and comprehend crimes with artificial intelligence. It enhances enterprises' cyber security to safeguard groups and customers from cybercriminals. In contrast, AI can be incredibly helpful. Not all uses are wise. Additionally, cybercriminals that use the generation to improve their cyber-attacks can use it as a new weapon. Cyber security synthetic intelligence helps safety personnel monitor and comprehend crimes. It enhances enterprises' cyber security to safeguard groups and customers from cybercriminals. In contrast, AI can be incredibly helpful. Not all uses are wise. Additionally, cybercriminals that use the generation to improve their cyber-attacks can use it as a new weapon. The cyber security community is investing in AI. Hash it out. How AI cyber security enhances digital safety Location-perimeter, community, endpoint, software, and statistics security should have multiple tiers in modern businesses. Hardware or software firewalls and network security answers can track and allow or prohibit network connections. Once passed these safeguards, hackers will face your antivirus and antimalware solutions. They may encounter your IDS/IPS and others [3].

There are few literary resources on applying AI strategies to incident handling, but based on our enjoyment of the introduction of AI strategies in Tactical, and particularly Operational Cyber Intelligence, we've concluded that the main feature of AI in incident handling is solving a category challenge, i.e. the moder's unambiguous reference.

Over time, people have driven and completed the IR method. Cyber-attacks are now executed faster due to automation, making it hard for human analysts to keep up. Due to the volume and speed of automated cyberattacks, safety personnel often experience alert fatigue. Given its expertise in cyber security literature and products, AI is a promising solution. AI is also used to launch cyberattacks, necessitating AI-based defense to slow and stop them. However, the AI as a cyber assault target is equally significant. Over time, people have driven and completed the IR method. Cyber-attacks are now executed faster due to automation, making it hard for human analysts to keep up. Due to the volume and speed of automated cyberattacks, safety personnel often experience alert fatigue. Given its expertise in cyber security literature and products, AI is a promising solution. AI is also used to launch cyberattacks, necessitating AI-based defense to slow and stop them. However, AI as a cyberattack target is equally significant. [5].

2. Threat Detection and Response

Vulnerabilities in information security refer to the many different kinds of problems that can arise in any part of an information system, from the underlying hardware to the software. The whole information system is affected by these flaws, which make it difficult to run smoothly. They pose a serious threat to the system's availability, confidentiality, and integrity when used maliciously. As a result, research on security vulnerabilities is an essential part of information security [6]. Conventional security measures are unable to stop the proliferation of more sophisticated cyberattacks. As a result, companies are using AI into their cybersecurity plans to make them more effective. Artificial intelligence (AI) improves governance and compliance procedures, strengthens vulnerability management, and increases threat detection and response capabilities. Machine learning, deep learning, behavioral analytics, and natural language processing are some of the artificial intelligence (AI) tools that businesses can use to strengthen their cyber defenses and protect themselves from insider threats, phishing, malware, and other cyber dangers. The field of cyber security has found many uses using AI, such as [7]. By facilitating effective threat detection and response, AI is crucial to cyber security. Machine learning and natural language processing allow firms to sift through mountains of data in search of irregularities that can indicate cyber dangers. By analyzing network traffic for patterns and outliers, intrusion detection systems backed by AI algorithms can identify potential security breaches. Cyber threat hunting powered by AI also aids in locating and analyzing APTs that may be hiding inside networks. Supporting proactive defense strategies, predictive analytics further equips organizations to proactively identify and address potential threats before they materialize [7].

3. Security Incident and Defense Strategies

When the previously mentioned security factors—confidentiality, integrity, and availability—are compromised, it is known as a security incident. An individual or business could be affected by several forms of cyber occurrences, such as cyber threats and attacks [8]. A cyber-threat is an attempted security breach that could take advantage of a system's or asset's weakness, whereas an attack is the intentional and unlawful taking of such action. Some examples of cyber-attacks include viruses, data breaches, denial-of-service (DoS) assaults, and others.

Protecting computer systems and networks from threats that could compromise their data, software, or hardware or cause disruptions to the services they offer is the usual goal of cybersecurity defense measures. They are in charge of preventing security incidents, which include data breaches, which can be described as any type of hostile or illegal behavior, and protecting the systems [9]. What follows is a synopsis of the most common types of conventional security measures.

3.1. Access Control

One security measure that is commonly used in computing environments is access control [10], which controls who may access and how they can utilize resources including data, system files, and computer networks. To reduce risk to the organization or entity, an attribute-based or role-based access control scheme can be employed, for instance, to limit network access based on individual users' responsibilities.

3.2. Firewall

The term "firewall" refers to a network security structure that monitors and controls data packets entering and leaving the network. To accept or prohibit traffic, firewalls use a predefined set of security rules and can be either host-based or network-based. To prevent attacks like malicious traffic, it can also filter traffic from unsecured or suspected sources [11].

3.3. Antimalware

Software that can identify, block, and remove malicious software from a computer system is called anti-malware [12]. Antivirus software nowadays can safeguard users from a wide range of malicious software threats, including spyware, trojan horses, worms, ransomware, and backdoors.

3.4. Sandbox

By physically isolating each process, a sandbox [13] can prevent system crashes or software vulnerabilities from affecting other processes. The execution of programs or code from unverified sources, such as suppliers, users, websites, or third parties, is a common use case for this.

3.5. Security information and event management (SIEM)

By fusing SIM with SEM, a system known as security information and event management (SIEM) [14] may analyze security warnings for devices and networks in real-time.

3.6. Cryptography

In order to encrypt and decrypt data for communication, cryptography [15] makes use of secret keys, such as secret-key, public-key, and hash functions.

Even though well-known, conventional security methods have their uses, they may not be up to the task of meeting the varied demands of the modern cyber business due to a lack of intelligence and adaptability [16, 17, 18, 19]. An increasingly used security measure is the intrusion detection system (IDS), which is "a device or software application that monitors a computer network or systems for malicious activity or policy violations" [20].

4. Challenges of AI in Cyber Security

There are several obstacles and drawbacks that hinder the advancement of AI in cybersecurity, notwithstanding its benefits. A greater use of AI in cybersecurity has been hindered by its limitations and downsides.

AI and its usability by Criminals

The use of AI by cybercriminals is the primary concern. As a result, AI has both positive and negative aspects. Because cybercriminals can easily acquire AI systems and analyze them for weaknesses, this technology is seen as a constraint. Their attacks will be more targeted and effective as a result of this action. Big data and spark engines have made it easier than ever to use AI models to analyze unstructured data for security dangers [21].

AI Adaptability in an Organizational Setup

Concerns about how to implement AI in cybersecurity have also been a major roadblock. AI is a relatively young technological development. Very few people understand the possibilities of AI. Most corporations have been hesitant to accept the technology because of how quickly it is growing [22]. AI is another area where these companies will need to pour a lot of money. Most organizations may find it difficult to adopt due to the expense. Therefore, their popularity in cybersecurity is likewise shallow due to the limited technology. To overcome this obstacle, more people must learn about the possibilities of this technology. This will encourage additional study into the field of artificial intelligence and help spread its use.

Cybersecurity protection systems still find AI to be a caring technology, despite the limitations and concerns mentioned before. Various types of attacks have allegedly been thwarted by the technology. It is possible to include the technology into a cybersecurity system so that it can resist various forms of seizures. Specialists can now be hired at a lower cost due to this feature. The technology's incapacity to make mistakes comparable to humans makes it the ideal candidate for building a robust defense.

5. Conclusion and Future Scope

AI is playing an increasingly important role in cybersecurity, offering numerous benefits such as enhanced threat detection, reduced false positives, automation, improved response time, and predictive analytics. However, challenges such as lack of transparency, bias, adversarial attacks, integration, and skill gap must be addressed. Organizations should consider ethical and regulatory frameworks when implementing AI-driven security solutions and adopt a holistic approach to cybersecurity that combines AI with traditional security techniques. By staying ahead in the AI arms race, organizations can better protect their networks from ever-evolving cyber threats.

References

1. Kemmerer, R. A. (2003). Cyber security. 25th International Conference on Software Engineering, 2003.
2. C.Felix. Freiling Laboratory for Dependable Distributed Systems University of Mannheim, Bastian Schwittay Symantec (Deutschland) GmbH.
3. LJUBOMIR LAZIĆ Belgrade Metropolitan University, Faculty of Information Technologies, BENEFIT FROM AI IN CYBERSECURITY the 11th International Conference on Business Information Security, 18th October.
4. R.Trifonov, R.Yoshinov, S.Manolov, G.Tsoche, & G.Pavlova. Artificial Intelligence methods are suitable for Incident Handling Automation. MATEC Web of Conferences, 292, 01044.
5. Vasileios Anastopoulos, PhD Davide Giovannelli, LL. M./05/2022/Automated/ Autonomous Incident Response [Online]. Available: https://www.bath.ac.uk/publications/li-brary-guides-to-cit-ing-referencing/attachments/ieee-styleguide.pdf
6. Q. Zhu, L. Liang, “Research on Security Vulnerabilities Based on Artificial Intelligence,” in ICIC, 2019, pp. 377-387.
7. S. A. Jawaid, “Artificial Intelligence with respect to Cyber Security,” Vienna, USA, 2023.
8. Nan Sun, Jun Zhang, Paul Rimba, Shang Gao, Leo Yu Zhang, and Yang Xiang. Data-driven cybersecurity incident prediction: A survey. IEEE Communications Surveys & Tutorials, 21(2):1744{1772, 2018.
9. Ansam Khraisat, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2(1):20, 2019.
10. Hui Qi, Xiaoqiang Di, and Jinqing Li. Formal definition and analysis of access control model based on role and attribute. Journal of information security and applications, 43:53-60, 2018.
11. Jun Yin. Firewall policy management, May 10 2016. US Patent 9,338,134.
12. Yinxing Xue, Guozhu Meng, Yang Liu, Tian Huat Tan, Hongxu Chen, Jun Sun, and Jie Zhang. Auditing antimalware tools by evolving android malware and dynamic loading technique. IEEE Transactions on Information Forensics and Security, 12(7):1529-1544, 2017.
13. Tyler Hunt, Zhiting Zhu, Yuanzhong Xu, Simon Peter, and Emmett Witchel. Ryoan: A distributed sandbox for untrusted computation on secret data. ACM Transactions on Computer Systems (TOCS), 35(4):1-32, 2018.
14. Muhammad Irfan, Haider Abbas, Yunchuan Sun, Anam Sajid, and Maruf Pasha. A framework for cloud forensics evidence collection and analysis using security information and event management. Security and Communication Networks, 9(16):3790-3807, 2016.
15. Omar G Abood and Shawkat K Guirguis. A survey on cryptography algorithms. International Journal of Scientific and Research Publications, 8(7):410-415, 2018.
16. Shahid Anwar, Jasni Mohamad Zain, Mohamad Fadli Zolkipli, Zakira Inayat, Suleman Khan, Bokolo Anthony, and Victor Chang. From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. Algorithms, 10(2):39, 2017.
17. Sara Mohammadi, Hamid Mirvaziri, Mostafa Ghazizadeh-Ahsaee, and Hadis Karimipour. Cyber

intrusion detection by combined feature selection algorithm. Journal of information security and applications, 44:80-88, 2019.

18. Juan E Tapiador, Agustin Or la, Arturo Ribagorda, and Benjamin Ramos. Key-recovery attacks on kids, a keyed anomaly detection system. IEEE Transactions on Dependable and Secure Computing, 12(3):312-325,2013.
19. Mahbod Tavallaee, Natalia Stakhanova, and Ali Akbar Ghorbani. Toward credible evaluation of anomalybased intrusion-detection methods. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 40(5):516-524, 2010.
20. Leighton Johnson. Computer incident response and forensics team management: Conducting a successful incident response. 2013.
21. Dash, B. (2021). A hybrid solution for extracting information from unstructured data using optical character recognition (OCR) with natural language processing (NLP).
22. S. Lee, (2021). AI-based Cybersecurity: Benefits and Limitations. Robotics & AI Ethics, 6(1), 18-28.