How Artificial Intelligence (AI) Can Revolutionize Modern Cybersecurity

My Nguyen

Old Dominion University

CYSE 280 - Windows System Management and Security

Professor Gladden

April 17, 2025

Table of Contents

How Artificial Intelligence (AI) Can Revolutionize Modern Cybersecurity

Introduction

Among the many technological advances and social transformations, the term "artificial intelligence" has undoubtedly become the hottest topic in the last few years. Over the past two to three years, the acronym AI has appeared in numerous journal articles, business studies, and technical reports, and its English equivalent, AI, has firmly secured the title of "Word of the Year 2023", according to Collins English Dictionary (The Economic Times, 2023). AI is emerging as an indispensable ally in the ever-evolving battle against cyber threats. Whether it's proactive detection of suspicious activity, behavioral analysis, or automated response, AI is redefining the boundaries of digital security. As technology continues to evolve, effective integration of AI becomes essential to protect our data and systems against the growing challenges of the digital world.

Overview of the Research

With the rapid development and growth of information technology (IT), computer networks have penetrated every aspect of people's lives. Whether it is in daily life, work, or study, it is inseparable from the support of computer networks. However, the openness and sharing of the network environment also bring many security risks. Therefore, computer network security management is critical (Pramanik et al., 2022). First, computer network security management is crucial to protecting personal privacy. In the Internet age, personal information has become a vital resource. Once leaked or abused, it will cause huge losses to individuals. For example, the leakage of personal identity information may lead to identity theft, financial fraud and other problems. Therefore, strengthening computer network security management through encryption technology, access control, and other means can effectively protect personal privacy and prevent criminals from obtaining and using personal information.

Secondly, computer network security management is vital to maintaining national security. In modern society, computer networks have become an essential infrastructure for national operations involving multiple fields such as politics, economy, and military (Li & Liu, 2021). Once a computer network is attacked or destroyed, it will seriously impact national security. For example, hacker attacks may lead to the leakage or tampering of critical data and even trigger a cyber war between countries. Traditional network security management methods can no longer cope with increasingly complex and changing network threats (Li & Liu, 2021). Therefore, it is imperative to seek new technical means to improve and enhance the efficiency and accuracy of network security management. The rise of AI technology has brought new solutions to computer network security management. Moreover, by simulating human thinking and behavior processes, AI can discover patterns, identify anomalies in large amounts of data, and automate response processes, taking instant action to isolate compromised systems or block malicious activity.

Framework

As the computer's core software, the operating system manages hardware resources and provides a software operating environment. However, due to its complexity and diversity, there are inevitably some vulnerabilities and defects in the operating system. If hackers or other malicious attackers exploit these vulnerabilities, they pose a serious security threat to the computer system (Chng et al., 2022). First, hackers may exploit the operating system's vulnerabilities for various attacks. Hackers may use vulnerability detection tools to discover and exploit these vulnerabilities to invade the computer system (Pramanik et al., 2022). Once successfully invaded, hackers may implant malicious code, such as viruses and Trojans, to steal users' personal information, disrupt the system's normal operation, or even control the entire computer system. In addition, hackers may also exploit vulnerabilities in the operating

system to launch denial of service attacks, making the computer system unable to work properly causing huge losses to individuals and enterprises.

Different operating systems have different architectures, interfaces, and security policies, which requires security managers to formulate different security policies and management measures for each operating system (Pramanik et al., 2022). However, human and resource limitations make it difficult to ensure that each operating system can be fully protected. In this case, once a new vulnerability appears in a certain operating system, hackers may quickly exploit it and threaten the entire network.

Results

Traditional network security management methods often rely on fixed rules and patterns to filter and judge traffic. However, this static protection method seems to be stretched in the face of increasingly complex and changeable network attack methods. AI technology has made real-time network traffic monitoring and analysis more accurate and efficient (Kaur et al., 2023). First, AI can use algorithms such as deep learning to perform real-time network traffic analysis. By training and learning a large amount of network traffic data, AI can automatically identify the characteristics of normal and abnormal traffic and accurately determine which traffic may contain potential attack behaviors (Kaur et al., 2023). This data-driven analysis method is better, more accurate, robust, and flexible than the traditional rule-based method.

Sarker (2021) carried out a performance analysis of the Perceptron neural network, from which he revealed that this AI algorithm shows an improvement in the duration of the training, which is shorter. It allows the cybersecurity defense to be ready in a shorter time, and this time reduction does not influence the number of false positives detected. Through such studies, it is possible to observe that AI has been applied to implement information security in real-time threat detection in systems, thus allowing immediate actions to be taken

on intrusions (Ansari et al., 2022). In addition, AI not only allows action when the threat is already in the system but can also study and predict intrusion patterns, thus allowing decision-makers to establish measures against possible future data breach attacks, all this in an automated way.

Organizations have thousands of incidents to process in which real attacks are hidden. Security Operation Centers (SOCs) can then be overwhelmed by "false positives" that weigh on experts' workload. In this context, AI can free up time to manage and respond to attacks by providing better analysis. SOCs could thus benefit from automation in the sorting of alerts thanks to Robotic Process Automation (RPA) which analyzes data by comparing it to blacklists and other malware databases (Dhabliya et al., 2023). This technique is also essential for responding to incidents automatically by applying new rules to protect against threats. However, to determine the severity of incidents and sort false alerts from real attacks, RPA is not enough because it does not learn from its experience. AI-based cognitive automation uses Machine Learning (ML) to ensure this sorting (Ozkan-Okay et al., 2024). This is undoubtedly one of the most promising AI techniques in cybersecurity. Allowing algorithms to learn without pre-established rules and hours of training on vast data catalogues leads them to differentiate the pathological from the normal and respond accordingly.

AI can also monitor organizations' information assets through situational awareness. This cognitive automation method can detect threats that are still unknown in a company's environment. At this stage, the alliance of analysts with AI is fundamental to the success of this permanent monitoring. It is therefore necessary to review the processes for handling security incidents within companies to include AI as a real "stakeholder". The "next-generation antivirus" (NGAV) also represents opportunities to strengthen cybersecurity at the "End-Point" level (Wu et al., 2022). Offering complex analyses to identify illegitimate

behavior (for example, APT attacks), these NGAVs also advise users on actions to protect themselves better.

Another area where AI brings added value is regaining control of its information assets. In the context of GDPR compliance, organizations are taking advantage of this turning point to map their information, often scattered across their infrastructures (Folorunso et al., 2024). Per its understanding of the information patterns that can be submitted to it, AI, accompanied by machine learning, helps to identify data within the information system by proposing the application of sensitivity or confidentiality level "tags". AI and ML bring levels of analysis that the human mind cannot assimilate (Folorunso et al., 2024). Therefore, it is essential to start considering integrating these solutions to prepare the defense against these new waves of complex attacks that companies and organizations could be victims of.

Among the many aspects of computer network security management, firewalls and intrusion detection systems are two crucial lines of defense. Traditional firewalls often use static filtering rules and cannot make corresponding adjustments according to real-time changes in the network environment (Pramanik et al., 2022). An intelligent firewall can utilize AI technology to analyze real-time network traffic, deduce the features of normal and abnormal traffic, and make corresponding adjustments to protection strategies based on the analysis results. Therefore, this intelligent protection method can protect malicious traffic from passing through it and block further exploitation by hackers by attacking vulnerabilities. Moreover, the new generation of smart firewalls based on historical data and attack patterns will easily identify potential threats in advance (Kaur et al., 2023). By training and learning a large amount of network traffic data, intelligent firewalls can summarize the behavior patterns and rules of attackers and predict possible network threats in the future. Through reinforcement learning, AI enables adaptive defense strategies and optimized security configurations, and performs automated tests to identify vulnerabilities. This predictive

analysis can help network security managers formulate protection strategies in advance and promptly respond to potential security risks.

AI can also achieve real-time and comprehensive monitoring of the network system. Based on deep learning and machine learning technologies, intrusion detection systems can automatically identify abnormal behaviors and attack signs in the network system, send timely alarms, and take corresponding countermeasures (Lysenko et al., 2024). This method of intelligent intrusion detection greatly improves the efficiency and accuracy of network security management and protects network security. In addition, smart firewalls and intrusion detection systems can also work together to form a complete network security protection system (Dash et al., 2022). Smart firewalls are responsible for intercepting malicious traffic and preventing outside-in attacks; intrusion detection systems are for internal security status monitoring of the network system, finding out and responding to potential security risks in time. Both complement each other's strong points and coordinate to construct a powerful security defense line.

Conclusion

As digitalization progresses and becomes more widespread, cybersecurity becomes an important issue. Effective measures must be taken to ensure the integrity of computer systems and the data they contain. At the heart of this IT security revolution, AI is emerging as an essential tool with advanced solutions to detect, prevent and mitigate constantly evolving digital threats. Through automation and intelligence, AI can effectively improve the efficiency and accuracy of network security management and reduce security risks.

In summary, AI can be applied in the cyber industry to improve information security in several ways, such as the detection of malicious security attacks in real-time through the use of learning algorithms, thus seeking to reduce the predictability of the defense, and allowing the creation of software and security platforms with a very low response time. In

addition, AI can prevent attacks, where predictive modeling techniques can be used to analyze the stored data and thus predict possible threats. AI can also perform vulnerability analysis on systems and networks, which helps companies identify and correct weaknesses before attackers exploit them.

However, implementing this technology brings with it limitations that can represent challenges and risks for organizations, which are mainly related to the technical difficulty of its implementation, the low accessibility of the data that organizations usually offer would obstruct adequate analysis, the interpretation of the data carried out properly by the AI may cause mistrust among users, and the privacy rights of the data with which companies work may not be respected. As a recommendation to different companies and organizations, they should take advantage of AI's benefits in information security but carefully manage the risks involved. In future research, relevant personnel need to continue to pay attention to the development of AI technology and continuously improve and optimize related algorithms and models to ensure that they play a greater role in computer network security management. At the same time, interdisciplinary cooperation and exchanges should be strengthened to jointly promote innovation and development in computer network security management.

References

Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: A literature review. *International Journal of Advanced Research in Computer and Communication Engineering, 11*(9), 1-10. http://dx.doi.org/10.17148/IJARCCE.2022.11912

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and opportunities with AI-based cyber security intrusion detection: A review. *International Journal of Software Engineering & Applications (IJSEA)*, *13*(5), 13-22. http://dx.doi.org/10.5121/ijsea.2022.13502

Dhabliya, D., Ghule, G., Khubalkar, D., Moje, R. K., Kshirsagar, P. S., & Bendale, S. P. (2023). Robotic process automation in cyber security operations: Optimizing workflows with AI-driven automation. *Journal of Electrical Systems*, *19*(3), 96-106. https://www.researchgate.net/journal/Journal-of-Electrical-Systems-1112-5209

Folorunso, A., Adewumi, T., Adewa, A., Okonkwo, R., & Olawumi, T. N. (2024). Impact of AI on cybersecurity and security compliance. *Global Journal of Engineering and Technology Advances*, *21*(01), 167-184. https://gjeta.com/sites/default/files/GJETA-2024-0193.pdf

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., & Tatarchenko, Y. (2024). The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. *Economic Affairs*, *69*, 43-51. https://ndpublisher.in/admin/issues/EAv69n1f.pdf

Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. *IEEE Access*, *12*, 12229-12256. https://www.sciencedirect.com/science/article/pii/S2187050924034100/pdf?md5=8e737e29327d337c75a5086ee220db34&pid=1-s2.0-S2187050924034100-main.pdf

Pramanik, S., Samanta, D., Vinay, M., & Guha, A. (Eds.). (2022). *Cyber Security and Network Security*. John Wiley & Sons. https://www.researchgate.net/publication/359509679_Cyber_Security_and_Network_Security

The Economic Times. (2023). *Word of the year: 'AI', 'Rizz', 'Authentic' among top expressions that defined 2023*. https://economictimes.indiatimes.com/magazines/panache/word-of-the-year-ai-rizz-authentic-among-top-expressions-that-defined-2023/oxford-dictionary/slideshow/105752786.cms

Wu, Y., Ge, J., & Li, T. (2022). *AI and Machine Learning for Network and Security Management*. John Wiley & Sons. https://colab.ws/articles/10.1002%2F9781119835905