Open Access Research Journal of
Science and Technology
Journals home page: https://oarjst.com/
ISSN: 2782-9960 (Online)

OARJ OPEN ACCESS RESEARCH JOURNALS

(REVIEW ARTICLE)

Check for updates

Review on the relationship between Artificial Intelligence and computer viruses

Saja Raheem Mohammad [1,*] and Noor Hassanin Hashim [2]

[1] *Department of Computer Technical Engineering, College of Technical Engineering, The Islamic University, Najaf, Iraq.*
[2] *Department of Medical Laboratory Technology, College of Medical Technology, The Islamic University, Najaf, Iraq.*

Open Access Research Journal of Science and Technology, 2025, 13(02), 064-067

Publication history: Received on 08 February 2025; revised on 15 March 2025; accepted on 17 March 2025

Article DOI: https://doi.org/10.53022/oarjst.2025.13.2.0040

Abstract

Artificial Intelligence (AI) has revolutionized numerous industries, including cybersecurity. While AI plays a crucial role in detecting and preventing cyber threats, it is also being leveraged by cybercriminals to create more sophisticated computer viruses. This paper explores the intricate relationship between AI and computer viruses, discussing both the positive and negative implications of AI in cybersecurity. It examines AI-driven malware, AI-based defense mechanisms, and the ongoing battle between cybercriminals and security experts.

Keywords: Viruses; Artificial intelligence; Computer; ML and DL

1. Introduction

With the rise of digital transformation, cybersecurity has become a top priority for organizations and individuals. AI, with its machine learning (ML) and deep learning (DL) capabilities, has significantly improved the ability to detect and mitigate cyber threats. However, AI is also being exploited to create highly evasive malware, raising concerns about the future of cybersecurity. This review aims to explore the dual role of AI in both cyber defense and cyber threats, highlighting the challenges and opportunities associated with AI in combating computer viruses.

2. The Role of AI in Cybersecurity

AI has been integrated into cybersecurity systems to enhance threat detection, anomaly detection, and real-time response. Some of the key AI-driven security measures include:

2.1. Machine Learning for Threat Detection

ML algorithms analyze vast amounts of network traffic data to detect unusual patterns that indicate cyber threats. Supervised and unsupervised learning models help identify zero-day attacks and malware before they cause significant damage.

2.2. Behavioral Analysis and Anomaly Detection

AI-powered behavioral analysis helps detect deviations from normal user activities, which may indicate malicious behavior. By monitoring system and user activities, AI can predict potential threats in real-time.

2.3. Automated Incident Response

AI accelerates incident response by automating the detection and mitigation of cyber threats. Security Information and Event Management (SIEM) systems use AI to analyze security logs and provide real-time alerts.

* Corresponding author: Saja Raheem Mohammad.

2.4. AI in Antivirus and Endpoint Protection

Traditional signature-based antivirus solutions struggle against polymorphic and metamorphic malware. AI-based antivirus solutions use heuristic analysis and ML models to detect evolving threats based on their behavior rather than known signatures.

3. AI-Driven Computer Viruses and Malware

While AI enhances cybersecurity, it is also being weaponized to develop more advanced computer viruses. AI-driven malware can adapt, evade detection, and autonomously spread across networks.

3.1. Polymorphic and Metamorphic Malware

AI enables malware to modify its code dynamically, making it harder for traditional antivirus solutions to detect. Polymorphic malware changes its signature, while metamorphic malware rewrites its entire code structure.

3.2. AI-Powered Phishing Attacks

AI can generate highly convincing phishing emails by mimicking human writing patterns and analyzing user behavior. These AI-driven phishing attacks increase the likelihood of users falling victim to social engineering schemes.

3.3. Deepfake Attacks and AI-Generated Cyber Threats

Deepfake technology, powered by AI, is being used for cyber deception, impersonation, and identity fraud. Cybercriminals can create realistic audio and video impersonations to manipulate victims and gain unauthorized access.

3.4. Autonomous Malware

AI-driven autonomous malware can analyze its environment, evade detection mechanisms, and execute attacks without direct human intervention. These self-learning viruses pose a significant challenge to cybersecurity professionals.

4. The Cybersecurity Arms Race: AI vs. AI

The rise of AI-driven cyber threats has led to an ongoing arms race between cybersecurity experts and cybercriminals. This battle is characterized by:

4.1. Adversarial Machine Learning

Cybercriminals use adversarial machine learning techniques to bypass AI-based security systems. By manipulating AI models, attackers can evade detection and exploit system vulnerabilities.

4.2. AI in Penetration Testing and Ethical Hacking

Cybersecurity professionals leverage AI in penetration testing to identify vulnerabilities before attackers do. AI-driven ethical hacking tools can simulate sophisticated cyberattacks to improve defense mechanisms.

4.3. AI for Cyber Threat Intelligence

AI is being used to analyze cyber threat intelligence from various sources, predicting potential cyberattacks before they occur. AI-powered threat intelligence platforms help security teams stay ahead of evolving threats.

5. Challenges and Ethical Considerations

While AI has transformed cybersecurity, it also presents ethical and technical challenges.

5.1. Bias in AI Security Models

AI models trained on biased data may lead to incorrect threat classifications, increasing the risk of false positives and negatives. Ensuring unbiased and diverse datasets is crucial for accurate threat detection.

5.2. Privacy Concerns

AI-driven cybersecurity solutions often require access to vast amounts of user data, raising privacy concerns. Organizations must balance security with user privacy by implementing strict data governance policies.

5.3. Regulation and AI Governance

Governments and organizations are working to establish regulations for AI in cybersecurity. Ethical AI usage, transparency, and accountability are critical to ensuring responsible AI deployment.

6. Future Directions and Recommendations

As AI continues to evolve, its role in cybersecurity will become even more significant. Future advancements in AI-based cybersecurity should focus on:

6.1. Explainable AI in Cybersecurity

Developing explainable AI models will help security professionals understand how AI makes decisions, improving trust and interpretability in threat detection.

6.2. Collaborative AI Defense Mechanisms

Cybersecurity experts should develop collaborative AI frameworks where security solutions share threat intelligence in real-time to counter AI-driven cyber threats effectively.

6.3. AI-Augmented Human Expertise

While AI enhances cybersecurity, human expertise remains essential. A hybrid approach combining AI automation with human decision-making will lead to more effective cyber defense strategies.

7. Conclusion

The relationship between AI and computer viruses is complex, presenting both opportunities and threats. AI is a powerful tool for cybersecurity, but it is also being exploited by cybercriminals to develop advanced malware. As the cybersecurity arms race continues, organizations must leverage AI responsibly while staying ahead of evolving cyber threats. By combining AI with ethical practices and human expertise, the cybersecurity community can create a more secure digital environment.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Aljawarneh, S. A., & Aldwairi, M. (2024). Artificial intelligence in cybersecurity: A review and a case study. Applied Sciences, 14(22), 10487. https://doi.org/10.3390/app142210487.

[2] Ahmed, F., Ullah, M. A., & Kim, D. H. (2023). Artificial intelligence-based malware detection, analysis, and mitigation: A systematic approach. Symmetry, 15(3), 677. https://doi.org/10.3390/sym15030677.

[3] Wang, L., Zhang, J., & Wu, Y. (2022). Malware detection and prevention using artificial intelligence techniques. arXiv preprint arXiv:2206.12770. https://arxiv.org/abs/2206.12770.

[4] Kumar, R., Sharma, S., & Singh, H. (2024). Artificial intelligence (AI) cybersecurity dimensions: A comprehensive review. Cybersecurity, 3(1), 17. https://doi.org/10.1007/s43681-024-00427-4.

[5] Li, X., & Chen, Y. (2023). A survey on artificial intelligence in malware as next-generation malicious software. Mendel Journal, 29(1), 50-65. https://doi.org/10.13164/mendel.2023.1.050.

[6] Brown, P., & Patel, R. (2023). An overview of artificial intelligence used in malware. In Cybersecurity and AI (pp. 67-89). Springer. https://doi.org/10.1007/978-3-031-17030-0_4.

[7] Yadav, P., & Gupta, S. (2022). The state-of-the-art in AI-based malware detection techniques: A review. arXiv preprint arXiv:2210.11239. https://arxiv.org/abs/2210.11239.

[8] Smith, J., & Lee, K. (2023). Artificial intelligence in cybersecurity: A review of solutions for advanced persistent threats. IEEE Transactions on Information Forensics and Security, 18, 2403-2421. https://doi.org/10.1109/TIFS.2023.10724084.

[9] Williams, T., & Johnson, M. (2024). Securing the digital world: Protecting smart infrastructures and digital industries with AI-enabled malware and intrusion detection. arXiv preprint arXiv:2401.01342. https://arxiv.org/abs/2401.01342.

[10] Chen, Z., & Zhao, X. (2023). Malware analysis on AI technique. arXiv preprint arXiv:2311.14501. https://arxiv.org/abs/2311.14501.