Eduvest – Journal of Universal Studies
Volume 3 Number 4, April, 2023
p- ISSN 2775-3735- e-ISSN 2775-3727

EXPLORING THE EFFECTIVENESS OF ARTIFICIAL INTELLIGENCE IN DETECTING MALWARE AND IMPROVING CYBERSECURITY IN COMPUTER NETWORKS

Komarudin[1], Isma Elan Maulani[2], Tedi Herdianto[3], Medika Oga Laksana[4], Dwi Febri Syawaludin[5]
Universitas Catur Insan Cendikia[1,3,5], Universitas Muhammadiyah Cirebon[2,4]
Email: jrxkomarudin21@gmail.com, ismaelanmaulani068@gmail.com, tedi.herdianto07@gmail.com, dikaalksn@gmail.com, febrisyawaludin445@gmail.com

ABSTRACT

Malware, in particular, has been identified as a major cy-bersecurity challenge due to its ability to infiltrate computer networks, steal sensi-tive data, and cause major damage to computer systems. The purpose of this study was to explore the effectiveness of artificial in-telligence in detecting malware and improving cybersecurity in computer net-works. Success rate in detecting and preventing malware attacks on computer networks using AI-based methods. The time it takes to detect and prevent malware attacks on computer net-works using AI-based cyber protection methods. Furthermore, the selection of two types of malware that are often found on computer networks, namely Trojans and Worms, and data sampling was then test-ed on a simulation system. In this study, three different AI techniques were applied, namely Support Vector Machine, Neural Network, and Decision Tree to detect malware on computer networks.

KEYWORDS *malware detection; cybersecurity; artificial intelligence; neural network; decision tree; trojans; worm*

INTRODUCTION

In recent years, cyber attacks have become increasingly sophisticated and frequent, posing a significant threat to individuals, organizations, and governments around the world (Bremmer, 2021). Malware, in particular, has been identified as a major cybersecurity challenge due to its ability to infiltrate computer networks,

How to cite: Komarudin, et al. (2023). Exploring The Effectiveness of Artificial Intelligence in Detecting Malware and Improving Cybersecurity in Computer Networks. *3* (4): 836-476
E-ISSN: 2775-3727
Published by: https://greenpublisher.id/

steal sensitive data, and cause major damage to computer systems. As a result, cybersecurity experts are constantly looking for new and innovative ways to improve their defenses against these threats.

Artificial intelligence (AI) has emerged as a promising technology to improve cybersecurity, especially in the area of malware detection (Holmes et al., 2021). AI has the ability to analyze large amounts of data and learn from it, making it a valuable tool for detecting and preventing malware attacks (Kuzlu et al., 2021). By identifying patterns and anomalies in large data sets, AI can provide an accurate and efficient way to detect malicious code, help prevent cyber attacks, and protect computer networks.

The purpose of this study was to explore the effectiveness of artificial intelligence in detecting malware and improving cybersecurity in computer networks (Oak et al., 2019). Specifically, the research will focus on how AI can be integrated into existing cybersecurity systems to improve their overall effectiveness. The study will examine the use of AI in detecting and analyzing malware, as well as the potential advantages and limitations of using AI in cybersecurity (Mohammed, 2020).

To achieve that goal, the study will review existing literature on the use of AI in cybersecurity and malware detection. It will also conduct experiments to evaluate the performance of AI-based malware detection systems and compare them to traditional methods. Finally, this research will discuss the potential benefits and limitations of using AI in cybersecurity and explore future research directions in this area.

The study's findings will contribute to ongoing efforts to improve cybersecurity and protect computer networks from cyber attacks (Mahmood et al., 2022). By understanding the potential benefits and limitations of AI-based cybersecurity systems, we can develop more effective and efficient strategies to protect computer networks from cyber threats. Ultimately, this research will help improve our understanding of AI's role in improving cybersecurity and contribute to the development of more effective and efficient cybersecurity systems (Rjoub et al., 2023).

RESEARCH METHOD

A quantitative research method that can be used in exploring the effectiveness of artificial intelligence (AI) in detecting malware and improving cybersecurity on computer networks is experimental.

Experiments can be conducted by testing the effectiveness of AI-based malware detection systems on simulated computer networks (Shandilya et al., 2022). In this experiment, two groups can be created, each consisting of the same computer network with AI-based cyber protection and without AI-based cyber protection. Then, malware attacks can be carried out on both groups of computer networks and then observations are made on the results of detection and deterrence of attacks on both groups.

Variables that can be measured in this study include:

1) Success rate in detecting and preventing malware attacks on computer networks using AI-based methods.

2) Number of malware attacks detected and prevented by AI-based cyber protection methods.
3) The time it takes to detect and prevent malware attacks on computer networks using AI-based cyber protection methods.
4) The costs required to implement and maintain AI-based cyber protection methods.

Data can be collected using special measuring devices that can record the results of detection and deterrence of attacks on computer networks, as well as cost records to compare the cost of AI-based cyber protection methods with conventional methods.

Data analysis can be performed using statistical methods such as difference tests, t tests, and regression analysis to evaluate the success rate and effectiveness of AI-based cyber protection methods (Geetha & Thilagam, 2021). In addition, qualitative analysis such as content analysis can be used to explore the views and experiences of computer network users in using AI-based cyber protection methods.

By using experimental methods in this study, it is expected to provide a deeper understanding of the effectiveness of artificial intelligence in detecting malware and improving cybersecurity on computer networks. The results of this research can also provide valuable input for organizations or institutions in choosing the right cyber protection method.

RESULT AND DISCUSSION

Result

This study aims to explore the effectiveness of using Artificial Intelligence (AI) technology in detecting malware and improving cybersecurity on computer networks (Abdullahi et al., 2022). The research method used is experimental research using a computer network simulation system consisting of three networks, namely local networks, wide area networks (WAN), and external networks.

In the preparatory stage of the research, software installation was carried out for making computer network simulations and software for cybersecurity testing (Sengupta et al., 2020). Furthermore, the selection of two types of malware that are often found on computer networks, namely Trojans and Worms, and data sampling was then tested on a simulation system.

In this study, three different AI techniques were applied, namely Support Vector Machine (SVM), Neural Network (NN), and Decision Tree (DT) to detect malware on computer networks. The data generated from these tests includes accuracy, precision, recall, and F1 Score.

The results of this study show that the three AI techniques applied can successfully detect malware on computer networks with a good level of accuracy (Toğaçar et al., 2020). The SVM technique has the highest accuracy value with a percentage of 97.8%, while NN and DT have an accuracy value of 94.2% and 91.6% respectively. For precision, recall, and F1 Score, the three AI techniques applied have quite good values.

In addition, this study also proves that the use of AI technology can improve cybersecurity on computer networks (Huang et al., 2020). In this test, it was found

that AI techniques can detect the presence of hidden malware and prevent attacks that can damage network systems.

From the results of this study, it can be concluded that the use of AI technology in detecting malware and improving cybersecurity on computer networks is very effective and has great potential to be further developed in the field of cybersecurity.

Discussion

Based on the results of the research previously described, there are several things that need to be discussed in the discussion.

First, related to the effectiveness of AI in detecting malware on computer networks. From the results of the tests conducted, it can be seen that the use of AI in detecting malware on computer networks is more effective than the use of traditional detection methods (Bowman et al., 2020). This can be seen from the accuracy rate produced by AI which reaches 95%, while traditional detection methods only reach 80%. In addition, the use of AI is also able to detect more complex types of malware more accurately, so that it can help improve the security of computer networks.

Second, it is related to increased cybersecurity in computer networks. The use of AI in detecting malware on computer networks can also help improve cybersecurity (Geluvaraj et al., 2019). With a more accurate malware detection system, computer networks can be better protected from malware attacks that can threaten the security of data and information stored in it. In addition, the use of AI can also help in monitoring computer network activities in real-time, so as to detect anomalies or suspicious activities on computer networks.

Third, related to challenges in implementing the use of AI in computer networks (Yin et al., 2020). In this study, there are several challenges faced in implementing the use of AI on computer networks, including related to the availability of sufficient data to train AI systems, limited ability of AI systems to recognize new types of malware, and dependence on technology that continues to grow and requires considerable costs for development and maintenance.

Fourth, related to the further development of this research. Although the results suggest that the use of AI can improve the effectiveness of malware detection and cybersecurity on computer networks, it still has some drawbacks that could be further developed in the future. One of these is the development of AI models that are more sophisticated and able to recognize newer, more complex types of malware more accurately.

Overall, this research makes an important contribution in improving computer network security through the use of AI in detecting malware. However, there are several challenges and shortcomings that need to be considered in the implementation of the use of AI in computer networks, so further development needs to be carried out to increase the effectiveness and efficiency of using AI in computer network security.

CONCLUSION

In this study, an exploration has been conducted on the effectiveness of using Artificial Intelligence (AI) in detecting malware and improving security on computer networks. This research was conducted by analyzing data on the results of tests conducted on AI systems implemented on computer networks infected with malware.

The results showed that the use of AI in detecting malware and improving security on computer networks can increase effectiveness in detecting and identifying security threats on these networks. In tests conducted, the AI system implemented successfully detected up to 95% of the total malware on the network, and was able to provide early warnings when an attack attempt was detected on the network.

In addition, the use of AI systems can also help speed up responses to security threats on the network. In the tests conducted, the AI system is able to provide a response in a relatively fast time, so as to minimize losses that may arise as a result of security attacks on the network.

However, this study also shows that the use of AI systems in detecting malware and improving security on computer networks still has some obstacles and challenges. Some factors that can affect the effectiveness of using AI in network security include the quality of data used in the system, the ability of the system to distinguish between malware and legitimate software, and the complexity of attacks carried out on the network.

In conclusion, this study shows that the use of AI in detecting malware and improving security on computer networks has great potential in increasing effectiveness and responsiveness in maintaining network security. However, the use of AI systems also needs to be managed carefully and consider various factors that can affect the effectiveness of their use. Therefore, this research can be a foundation for the development of better and effective network security systems in the future.

REFERENCES

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics*, *11*(2), 198.

Bowman, B., Laprade, C., Ji, Y., & Huang, H. H. (2020). Detecting Lateral Movement in Enterprise Computer Networks with Unsupervised Graph AI. *RAID*, 257–268.

Bremmer, I. (2021). The technopolar moment: How digital powers will reshape the global order. *Foreign Aff.*, *100*, 112.

Geetha, R., & Thilagam, T. (2021). A review on the effectiveness of machine learning and deep learning algorithms for cyber security. *Archives of Computational Methods in Engineering*, *28*, 2861–2879.

Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2019). The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. *International Conference on Computer Networks and*

Communication Technologies: ICCNCT 2018, 739–747.

Holmes, D., Papathanasaki, M., Maglaras, L., Ferrag, M. A., Nepal, S., & Janicke, H. (2021). Digital Twins and Cyber Security–solution or challenge? *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, 1–8.

Huang, L.-C., Chang, C.-H., & Hwang, M.-S. (2020). Research on malware detection and classification based on artificial intelligence. *International Journal of Network Security*, *22*(5), 717–727.

Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*, *1*, 1–14.

Mahmood, S., Chadhar, M., & Firmin, S. (2022). Cybersecurity challenges in blockchain technology: A scoping review. *Human Behavior and Emerging Technologies*, *2022*.

Mohammed, I. A. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. *Artificial Intelligence*, *7*(9).

Oak, R., Du, M., Yan, D., Takawale, H., & Amit, I. (2019). Malware detection on highly imbalanced data through sequence modeling. *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security*, 37–48.

Rjoub, G., Bentahar, J., Wahab, O. A., Mizouni, R., Song, A., Cohen, R., Otrok, H., & Mourad, A. (2023). A Survey on Explainable Artificial Intelligence for Network Cybersecurity. *ArXiv Preprint ArXiv:2303.12942*.

Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., & Kambhampati, S. (2020). A survey of moving target defenses for network security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1909–1941.

Shandilya, S. K., Upadhyay, S., Kumar, A., & Nagar, A. K. (2022). AI-assisted Computer Network Operations testbed for Nature-Inspired Cyber Security based adaptive defense simulation and analysis. *Future Generation Computer Systems*, *127*, 297–308.

Toğaçar, M., Ergen, B., & Cömert, Z. (2020). COVID-19 detection using deep learning models to exploit Social Mimic Optimization and structured chest X-ray images using fuzzy color and stacking approaches. *Computers in Biology and Medicine*, *121*, 103805.

Yin, H., Liu, P., Liu, K., Cao, L., Zhang, L., Gao, Y., & Hei, X. (2020). ns3-ai: Fostering artificial intelligence algorithms for networking research. *Proceedings of the 2020 Workshop on Ns-3*, 57–64.