Proceedings of the 2nd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/73/20240397

Review of artificial intelligence applications and technologies in cybersecurity

Zimeng Li

School of Software Engineering, Tongji University, Shanghai, China

lizimeng@tongji.edu.cn

Abstract. With the rapid development of information technology and network technology, the Internet not only brings a lot of convenient resources to people's lives but also brings potential threats to people's network security, and the development of artificial intelligence provides new solutions for network security governance. The article focuses on common problems in network security, systematically summarizes the network security solutions based on AI technology and the empowering effects brought in recent years, analyzes the application of AI technology in common security problems, summarizes the advantages of AI in the application of network security, and puts forward the potential problems and challenges. Overall, AI technology has improved the accuracy, scalability, reliability and performance of network security applications in practical applications, and will become an essential engine of empowerment in the future development of network security technology.

Keywords: Cybersecurity, Artificial Intelligence, Big Data, Cyber Technology.

1. Introduction

Since 1969, the Internet has flourished over the decades. From the initial military network ARPANET to today's World Wide Web, the Internet's impact on human life continues to expand. With the rapid development of the digital economy derived from the Internet, network security has gradually become an increasingly obvious governance problem in the process of the interconnection of all things and technological development of modern society and has gradually been emphasized by countries around the world. Network security is not only a problem in the communications industry, but also in more important areas such as social, economic and military security. Although countries around the world are constantly strengthening network security technology, and increasing investment in the field of network security, the development of network security technology is still lagging behind the pace of malicious use of network technology, the frequency of network threats, the adverse effects and the complexity of the protection of the escalating.

However, in recent years, with the development of artificial intelligence, artificial intelligence technology in the application of network security gives people a new way to solve network security threats. The term "artificial intelligence" first originated in August 1956; John McCarthy, Marvin Minsky, Claude Shannon and others in the United States at a meeting of Dartmouth College, the original definition of artificial intelligence: "the use of machines to mimic human learning and other aspects of intelligence ". Starting from the 1990s, the improvement of physical computing power has made artificial intelligence usher in rapid development, and now, the maturity of Internet technology, big data,

© 2024 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/73/20240397

cloud computing and other supporting technologies have made the development of artificial intelligence faster and faster, and the powerful learning and computational capabilities brought by artificial intelligence are being continuously applied to network situational analysis, computer vision, speech recognition, natural language processing and many other fields.Artificial intelligence technology has human-like logic capabilities, enabling machines to realize the knowledge of the physical world and achieve autonomous decision-making; its internal logic is to understand the world through data input or through sensors to perceive the environment, and then use pattern recognition to achieve data classification, clustering, regression and other analyses, and accordingly make the optimal decision-making recommendations. In recent years, artificial intelligence technology has also been widely used in network security protection, which can solve the problems of network intrusion, malware, phishing and spam.

Further, when artificial intelligence is applied to the field of cybersecurity, technologies such as machine automation and machine learning can effectively and efficiently help humans predict, sense and identify security risks, quickly detect and locate sources of dangers, analyze the causes of security problems and ways of hazards, and synthesize the knowledge base of the intelligent brain to judge and select the optimal strategy, take mitigation measures or resist threats, and even provide further mitigation and repair recommendations. This process will not only reduce people's burden of work, but will also reduce their need to take care of themselves. This process not only frees people from heavy, time-consuming and complex tasks, but also allows them to face changing risk environments and abnormal attack threat patterns faster and more accurately than people, and the flexibility and efficiency of comprehensive analysis is also higher.

2. Methodology

In order to promote the development of network security technology research, this paper mainly summarizes the empowering effect of artificial intelligence technology in network security problems.

Firstly, it categorizes and gives examples to illustrate the application of AI technology in common security problems, and then systematically summarizes the network security solutions based on AI technology and the empowering effects brought by AI technology in recent years, points out the advantages of AI technology in its application, and puts forward the problems and challenges faced by AI technology in its future network security application.

3. Specific strategies of artificial intelligence in cybersecurity applications

3.1. Intelligent intrusion detection technology

In computer network security prevention, there is still some difficulty in detecting some complex and high levels of attack malicious code. Therefore, in order to further prevent malicious code attacks on the computer network system, it is necessary for technicians to analyze the abnormal conditions of the computer network system promptly, and to find out the existence of some potential threat factors in the computer network system.

The traditional network threat detection method based on feature rules is prone to a large number of false alarms, omissions and long delays in the face of complex network behavior and massive high-latitude big data environment. Since intrusion detection is based on network traffic data or host data to determine normal or abnormal behavior, it belongs to the classification problem, while artificial intelligence algorithms, such as machine learning, have a solid ability to solve the classification problem.

Combined with the current rapid development of artificial intelligence technology, intelligent intrusion detection is substantially optimized in terms of both detection capability and speed compared with traditional intrusion detection methods. In the field of network intrusion detection, in 2016, MIT's Computer Science and Artificial Intelligence Laboratory and startup Pattern jointly developed the AI (Artificial Intelligence + Analyst Intuition) system, which is an artificial intelligence-based network security intrusion detection platform. The system uses unsupervised machine learning to autonomously scan the content of log data and feed the clustering results to a human analyst. The human analysts will

DOI: 10.54254/2755-2721/73/20240397

identify which are real cyber-attack activities and continuously label the data of cyber-attack behaviors, and then give feedback on the results to the AI through supervised machine learning to upgrade the existing model, based on the principle of feedback loop, which is able to continuously improve the detection rate with more time and data volume.

The application of AI technology can provide technicians with a blueprint of the computer network system as well as information about the knowledge base involved, so that AI technology can be used to improve and optimize the defense system, resist the attacks caused by malicious code and other viruses on the computer network system, and better deal with computer network security incidents.

3.2. Spam detection technology

Most security threats use email as an attack vector. Traditional spam detection methods mainly set up rules on the mail server side for filtering and detection, and their rules are set up by configuring black and white lists with features such as IP address/IP network segment of the sending side, mail domain address, mailbox address, email subject or content keywords, etc. This method can only detect known spam, and the rule update has a lagging effect and low detection efficiency.

Therefore, the use of artificial intelligence technology to automatically update rules can effectively solve the shortcomings of traditional spam detection methods, and the classification of email text through the use of artificial intelligence learning algorithms is the current mainstream solution. For example, in June 2017, Google said that its recognition rate of spam and phishing emails based on intelligent machine learning technology had reached 99.9%. At the same time, according to Google's official data, 50% to 70% of the emails received by Gmail are spam, which provides a steady stream of high-quality data sources for the training of intelligent machine learning models. Then combined with Google's algorithmic and data processing capabilities, real-time updating of the spam detection model has been achieved.

3.3. Intelligent firewall technology

Firewalls are the main security devices currently used to protect computer networks. As a kind of isolation control technology, a firewall establishes a barrier between the internal network and the insecure external network, preventing illegal access to the internal network from the outside and, at the same time, preventing important information from flowing out of the internal network.

In the traditional network security defense mechanism, in the existence of a variety of firewalls, but such firewall applications have not reached the user to use the ideal effect, it is difficult to achieve a comprehensive defense against network security risks. Its working principle is to set up some security rules in advance; if it meets the security rules, it is allowed to pass; if it does not meet the security rules, it is not allowed to pass, but in the actual use of the process, if the security software is not within the firewall rules set, it will not be passed, and then affect people's work and life. It can be seen that the traditional firewall settings can play a certain role in protection, but the protection ability to set up a more rigid, can only be based on the initial settings for protection, but in the actual application of some of the safe and usable programs will be filtered out, which will have a certain negative impact on people's work and life.

The firewall based on artificial intelligence technology is very different, it not only has the ability to learn on its own, but also has a certain degree of autonomy to identify the ability to use a large amount of data to learn on its own to make an intelligent interception model, and then according to the actual situation of learning to amend, this adaptive identification of applications can be realized in the way of mobile access control. Unlawful elements attack computers by analyzing the vulnerability of firewalls. Traditional firewalls can not protect against such attacks, but intelligent firewalls can do timely protection, because they will update the model according to the actual situation, can intelligently identify new threats, and can effectively block computer viruses and network hacking, which is also the mainstream trend of the development of firewalls in the future.

DOI: 10.54254/2755-2721/73/20240397

3.4. Trojan horse virus detection and killing technology

Neural networks are complex structures but powerful processors, and the execution ability, calculation ability, fault tolerance and storage ability of neural networks are extremely strong, which can accurately recognize the information in cyberspace security. Therefore, in cyberspace security defense, the construction of a neural network system can effectively improve the performance of intelligent intrusion detection technology, promote the effective identification of information and viruses, reduce the error rate of the system's decision-making, and promote the effectiveness of the identification of information in the cyberspace, so as to enhance the level of big-data network security defense. For part of the Trojan virus hidden in the general App software, it can be analyzed in depth in a timely manner, so that the relevant viruses can be recognized by artificial intelligence in a timely manner, so as to avoid the virus from damaging the user's computer and important information.

3.5. Network data transmission encryption technology

In the context of artificial intelligence, the computer network system in the process of data transmission encountered in the process of more diversified problems. In order to better solve these problems, technicians should first rely on the computer network information system to carry out a comprehensive analysis, according to the computer network system in the process of data transmission of the specific problems encountered in the proposal of an effective solution strategy.

Computer network system for the process of data transmission, one of the main factors affecting data security is the encryption of data, computer network system, and some important documents and information in the transmission process through the implementation of encryption, in order to ensure the security of the entire transmission process. The encryption of data transmitted by the technicians to the computer network system can effectively solve the risk of theft or leakage of some personal information and other corporate information in the transmission process of the computer network system, and encryption add a layer of protective barrier to the information transmitted in the environment of the computer network system.

Based on the background of artificial intelligence, there are many widely used encryption technologies, such as fingerprint identification technology, facial recognition technology, voice recognition technology, intelligent paste recognition technology, etc. Through these different identification technologies, the safe transmission of relevant data in the computer network system is guaranteed, and the security protection of the risk of information transmission in the computer network is increased.

3.6. Patch updating and vulnerability checking technology

Technicians play a crucial role in preventing security risks in computer network systems. They need to ensure timely updates of patch programs to monitor and defend against computer virus attacks effectively. Real-time inspection of vulnerabilities in the operation of the computer network system can increase the strength of computer network monitoring and further improve its effectiveness.

Through real-time monitoring of the artificial intelligence network, it is possible to carry out rapid statistics and analysis of the relevant data in the operation of the intelligent network system, and according to the results of the analysis of the effective risk prevention strategy, check the vulnerabilities that exist in the artificial intelligence network, and according to the results of the inspection of the timely updating of the patching program, so as to further improve the level of protection against security risks in the computer network system.

4. Benefits and potential of artificial intelligence in cybersecurity applications

4.1. Fuzzy information processing capability

In the process of using network terminals, users usually browse all kinds of content and information, and there may be network viruses lurking under fuzzy information. Then network viruses can be successfully disguised with the help of such fuzzy information. In the detection of fuzzy information,

DOI: 10.54254/2755-2721/73/20240397

other network security technologies stay more on the surface, rarely able to comprehensively analyze the composition of fuzzy information, words and content, so fuzzy information may be hidden network viruses that are naturally difficult to find. Once the fuzzy information carrying network viruses successfully enters the network terminal, it will inevitably lead to different degrees of network security threats. However, with the help of artificial intelligence technology, it is possible to analyze fuzzy information from unknown sources by means of reasoning, and then analyze the content, volume, and other relevant parameters of the fuzzy information in-depth, so as to identify the type of information and the source of the information effectively, and then, through the search of information of the same source, it is possible to realize clear processing of such information, and according to the type of information, the relevant report will be sent to the terminal. In this way, end-users can avoid the threat of ambiguous information in advance after receiving the report.

4.2. Strong collaborative capability

The development of the Internet is very rapid, which can be easily seen from today's volume, and such a colossal volume will inevitably make the network scale become more huge, and its structure will become more and more complex, thus making the network security management will face the management difficulty will continue to increase, relying only on the existing network security technology has been difficult to achieve a more comprehensive network security protection. In such a development situation, a new management concept - that is, the concept of hierarchical management was born, and in the network security management work has been applied, so that the network security puts forward new management needs, and artificial intelligence technology with its strong collaborative ability can be very good to meet this demand.

4.3. Unique learning reasoning capability

Learning and reasoning ability is the most crucial ability of AI technology, with the help of which it can help AI technology in network security management to continuously learn from the network security problems that have already occurred and reason about the network security problems that may be about to occur. The total amount of information on the Internet is very large, which also leads to certain similarities and correlations between the information, and at this time, it is necessary to analyze and summarize the information with the help of reasoning ability, so that the relevant data that can provide reference can be extracted to provide the necessary data support for the development of network security management, and help the network security management work to be better carried out.

4.4. Low cost of network data computation

The cost of network data computing will have a direct impact on the benefits of the enterprise itself. In order to effectively control the cost of the enterprise, it is necessary to do a good job of the relevant network security control work. The traditional manual computing methods cause a waste of resources, time and energy consumption, which is also relatively large, the efficiency of data computing is low, which makes the network system's operating costs increase in an invisible way. The increase in enterprise costs represents the increasing cost of production and operation, which will have a negative impact on the development as well as optimization of the economic system. The use of artificial intelligence technology makes it possible to improve the level of network security and defense capabilities, and many optimized algorithms are used in practice, so that the data and information of different boards are effectively integrated and utilized, and the overall efficiency of the work can be comprehensively improved. Thus, the use of artificial intelligence technology makes the overall effect of network data configuration optimized.

5. Risks and challenges of artificial intelligence in cybersecurity applications

Artificial intelligence in the development of the application of its own also has some security risks, mainly including artificial intelligence framework security, algorithm security and data security.

DOI: 10.54254/2755-2721/73/20240397

5.1. Framework security

Many open-source AI programming frameworks and commercial AI programming frameworks have emerged in the market, providing users with a large number of highly reusable algorithms and modules, which integrate data cleaning, model construction, process editing, model tuning, and model evaluation. To provide developers with convenient AI applications. Mainstream frameworks include Caffe, Torch, TensorFlow, CNTK, Keras and so on. However, these frameworks themselves more or less have some security risks, vulnerable to network attacks. For example, there is a heap overflow vulnerability in the XLA compiler of TensorFLow before version 1.7.1, and the image vision inventory of Caffe framework has a vulnerability that can cause the program to crash.

5.2. Algorithm security

The core of artificial intelligence is algorithms, but the algorithms themselves have interpretability problems. The emergence of adversarial samples proves the lack of interpretability of artificial intelligence algorithms. For example, although the deep neural network can solve complex problems such as image recognition, machine translation, etc., its algorithm itself has poor interpretability; KNN algorithm is also insufficient in terms of interpretability, for example, different choices of K value will have a very different impact on the results of data classification.

5.3. Data security

Data is the raw material for AI algorithms to carry out training, and the quality of the dataset can have a fatal impact on the performance of the model. Many of the sample data used for training are collected online, and it is easy for an attacker to construct some illegal and misleading data to interfere with the data, which can cause the machine learning model to overfit or completely fail. For example, modifying only 8% of the sample data can lead to dose prediction errors in artificial intelligence models for drug dose prediction. In addition, some network attackers, in order to achieve malicious code free kills and malware concealment, began to use artificial intelligence technology against artificial intelligence network security defense systems, this attack is called "against machine learning". Adversarial machine learning technology can, through a certain algorithm, their own malicious samples and normal samples for fusion mutation in order to retain their own malicious behavior on the basis of bypassing the depth of detection based on machine learning, marking themselves as normal samples. Adversarial machine learning poses new challenges to network defense, therefore, while massively utilizing AI technology for network security protection, models and methods need to be continuously optimized and upgraded in order to cope with the endless network security threats.

6. Conclusion

With the ever-changing development of network technology, while providing people with various conveniences continuously, network security problems also emerge one after another, and it is very necessary to strengthen network security management and prevention.

This paper summarizes the latest progress in the application of artificial intelligence technology in the field of network security, involving technologies such as traditional machine learning, deep learning and reinforcement learning methods, investigates the relevant applications of artificial intelligence technology in the field of network security in recent years, and introduces the application scenarios of artificial intelligence technology in specific research directions. Finally, this paper points out the advantages of the current applications, as well as the problems and challenges faced in the future.

References

[1] Chen J, Wu D D and Xie R Y 2023 Artificial intelligence algorithms for cyberspace security applications:a technological and status review. *Frontiers in Information and Electronic Engineering (English Edition)* 24(8) 1117-1142. DOI:10.1631/FITEE.2200314

[2] Peng Z F, Xing G Q and Chen X Y 2022 An overview of the application and technology of artificial intelligence in the field of network security. *Information Security Research* 8(2) 110-116. DOI:10.12379/j.issn.2096-1057.2022.02.01

[3] Tusunjiang M 2022 Research on the application of artificial intelligence technology in big data network security defense. *Wireless Interconnection Technology* 19(11) 23-25. DOI:10.3969/j.issn.1672-6944.2022.11.008

[4] Song Y 2023 Application of artificial intelligence technology in network security defense. *Science and Technology Wind* 2023(6) 65-67. DOI:10.19392/j.cnki.1671-7341.202306022

[5] Zan J J 2022 Application of artificial intelligence in computer network security. *Network Security Technology and Application* 2022(4) 175-176. DOI:10.3969/j.issn.1009-6833.2022.04.101

[6] Pan Y L 2021 Research on network security management based on artificial intelligence. *Network Security Technology and Application* 2021(4) 5-7

[7] Charmet F, Tanuwidjaja H C, Ayoubi S, Gimenez P F, Han Y F, Jmila H, Blanc G, Blanc G, Takahashi T, Zhang Z H 2022 A review of research on interpretable artificial intelligence for network security. *Journal of Telecommunications* 77(11/12) 789-812.DOI: 10.1007/s12243-022-00926-7

[8] Sagar S, Murat K and Chen H C 2020 Trailblazing the Artificial Intelligence for Cybersecurity Discipline: A Multi-Disciplinary Research Roadmap. *ACM Transactions on Management Information Systems* 11(4) 17.1-17.19. DOI:10.1145/3430360

[9] House D and Norman D 2020 Considerations for Artificial Intelligence in Cybersecurity. *51st Annual Conf. of the Decision Sciences Institute 2020, vol. 2. Decision Sciences in the Age of Connectivity: 51st Annual Conf. of the Decision Sciences Institute.*21-23 November 2020, Online.Decision Sciences Institute 2020 821-826

[10] Haykin S 2019 Artificial Intelligence Communicates With Cognitive Dynamic System for Cybersecurity. *IEEE Transactions on Cognitive Communications and Networking* 5(3) 463-475. DOI:10.1109/TCCN.2019.2930253

[11] Wang Y F, Li P Ch, Yi B and Wang X W 2021 Artificial intelligence empowered cyber security applications. *Journal of Guangzhou University (Natural Science Edition)* 20(2) 1-12. DOI:10.3969/j.issn.1671-4229.2021.02.001

[12] Wang H H 2022 Research on network security protection based on artificial intelligence technology. *Wireless Internet Technology* 19(14) 13-15. DOI:10.3969/j.issn.1672-6944.2022.14.005

[13] Wang L L 2022 Computer network security risk control in the context of artificial intelligence. *Network Security Technology and Application* 2022(9) 171-173. DOI:10.3969/j.issn.1009-6833.2022.09.087

[14] Hu J M 2023 Computer network security risk control in the context of artificial intelligence. *Digital Communication World* 2023(4) 186-188. DOI:10.3969/J.ISSN.1672-7274.2023.04.060