Research on Computer Network Risk Prevention and Control Technology in the Information Age

Yue Guo1, Liang Dong1,*, Lei Zheng1, Shuang Qiu1, Lei Li1, Xianfei Zhang1, Hang Gao2, Yintie Zhang3
1State Grid Hubei Electric Power Information and Communication Company
2Nanjing Data Foundation Technology Co., Ltd.
3Information Systems Integration Branch, NARI Technology Co., Ltd, China

*Corresponding author email: liangdong@sgcc.com.cn

Abstract. With the advancement of global informatization, cyber risk has become an important factor hindering the informatization process, and cyber security issues have become the focus of public attention. Computer network security incidents include viruses, Trojan horses, worms, network monitoring, hacker attacks, malware, phishing, botnets, etc. In order to help netizens to prevent network security incidents more effectively, in response to the characteristics of network risk prevention data management, network Research and design of risk prevention database and data warehouse. At present, the development of computer technology is very rapid, but there are still many problems in the security of computer networks. Therefore, in order to avoid these problems hindering the development of the computer, the author analyses and discusses the technology related to computer network security protection in the information age, hoping to solve the computer network security problems and make the computer network more secure.

Keywords: Information age, computer, security protection, computer network technology, artificial intelligence.

1. Introduction
The artificial intelligence part is mainly based on Mosquito artificial intelligence. The Mosquito project is open source. We can download the source code files on the official website, add or delete some functions according to our needs and deploy them on our own servers to complete artificial intelligence. The establishment of the server Mosquito connects with the client, publishes and subscribes to the message through the poll mode. In addition, the topic of the message is placed in the subscription tree. Assume that there are subscriber clients to tell the artificial intelligence that they want to subscribe to a topic, then artificial intelligence will query the entire subscription tree, find the topic that matches the subscriber's client subscription, and return it to the client, which ends the subscription. The main goal of big data is to achieve messaging for publishing, subscribing, and simple message push, some functions in Mosquito are not available. You can turn off these functions when deploying software, so the main modules we deploy include business processing modules,
access control modules, and data. Encryption module, theme design module. Let me introduce him separately. Our working mechanism and configuration process.

In the current era, computer network technology continues to develop. Communication technology and network technology not only increase the production rate of society, but also greatly change people's lives and improve people's living standards. Artificial intelligence is the future direction of the development of computer information technology. Through this technology, enterprises can improve their management level, increase the speed of development, and reduce labour costs. In addition, artificial intelligence can also be used in agriculture, industry and other industries to promote the transformation of industry and production methods. Artificial intelligence technology can be applied in computer network technology, strengthen the security management of computer network, and promote data processing and analysis. It is an indispensable and important part of the future development of computer network technology. The integration of artificial intelligence in computer network technology can not only improve the efficiency of computer information processing, but also enhance the flexibility of computers, and at the same time bring great convenience to people. In the context of the development of intelligence and informatization, artificial intelligence is bound to be more widely used in computer networks [1].

2. About artificial intelligence computers

2.1. The principle of artificial intelligence

The development of artificial intelligence requires the support of computer technology and network technology. The process of artificial intelligence technology requires the use of virtual technology to allow the system to continuously simulate people's thinking styles and behaviours to reach a certain number before artificial intelligence technology can be completed. Artificial intelligence technology is a very complex technology. The soldiers contain a lot of complex content, and they have common ground with many scientific technologies, such as linguistics, psychology, computer science, etc. Technical support. The reason why I want to develop artificial intelligence technology is to allow artificial intelligence to replace people to complete more complex operations, but still achieve the goal of saving enterprise human resources costs and improving work results. Figure 1 shows the principle of artificial intelligence.

![Artificial Intelligence (AI)](image_url)

**Figure 1.** The principle of artificial intelligence
2.2. Characteristics of artificial intelligence technology

2.2.1. Solve complex network problems. With the continuous improvement of modern science and technology, the characteristics of artificial intelligence technology are also diversifying. In the past, many unsolvable problems can be solved by artificial intelligence technology. For example, some operations cannot know the calculation model of their body, but by using artificial intelligence technology, they can fully grasp the information, and through the management of artificial intelligence technology, network management can be further guaranteed.

2.2.2. Continuously enrich and update data. Artificial intelligence technology is not static. Its ability to prepare for continuous learning can continuously incorporate a lot of new knowledge, process data with low computational difficulty, and then obtain some higher-level data. Due to the continuous learning function of artificial intelligence, the level of network management continues to increase, and the running speed will also continue to accelerate, while reducing the time for people to search through the network [2].

3. The positive effect of artificial intelligence on the development of computer network technology

3.1. Efficient handling of fuzzy information
Artificial intelligence can efficiently process fuzzy information and complete fuzzy operations by simulating human brain capabilities. Under the background of the era of big data, network operation and maintenance can be realized by information alone. Computer network technology is the basis of network operation and maintenance based on information. Today, with the rapid economic development, all fields of industry use computer network technology to optimize and innovate their own business systems and management models, and process, use and manage the massive data information generated during the development process. Traditional computer network technology does not have the function of fuzzy calculation, it is difficult to store massive data information, and artificial intelligence can make up for this shortcoming, the fuzzy algorithm is used to blur the data to the extent that it is almost consistent with the human brain, and does not need to be particularly large. Storage space can make information processing timelier and more effective. Therefore, artificial intelligence is conducive to the improvement of computer information processing capabilities to promote the development of computer network technology. Figure 2 shows the principle of fuzzy calculation.

Figure 2. Principles of Fuzzy Computing
Assuming that the time series samples are n-dimensional vectors, k continuous data samples can be expressed as $$(x_i, y_i), i = 1, 2, ..., k \in \mathbb{R}^n \cdot \mathbb{R}$$, and the linear function is also set to $f(x) = \omega \cdot x + b$. The optimization problem is converted to the minimum value $R(\omega, \xi, \xi^*) = \frac{1}{2} \omega \cdot \omega + C \sum_{i=1}^{k} (\xi_i + \xi_i^*)$, and the constraints are:

$$f(x_i) - y_i \leq \xi_i^* + \varepsilon, \quad i = 1, 2, ..., k$$

$$f(x_i) - y_i \leq \xi_i, \quad i = 1, 2, ..., k$$

$$\xi_i, \xi_i^* \geq 0, \quad i = 1, 2, ..., k$$  \hspace{1cm} (1)

Among them, $\frac{1}{2} \omega \cdot \omega$ can improve the generalization ability of support vector machines, $C \sum_{i=1}^{k} (\xi_i + \xi_i^*)$ is the penalty term, and $\varepsilon$ is the insensitive loss function. The same problem becomes the problem of solving convex quadratic optimization, and the Lagrange function is introduced:

$$L(\omega, b, \xi, \xi^*, a, a^*, \gamma, \gamma^*) = \frac{1}{2} \omega \cdot \omega + C \sum_{i=1}^{k} (\xi_i + \xi_i^*)$$

$$- \sum_{i=1}^{k} a_i^* | \xi_i + \varepsilon - y_i + f(x_i) | - \sum_{j=1}^{k} a_j | \xi_j + \varepsilon - y_j + f(x_j) | - \sum_{i=1}^{k} (\gamma_i + \gamma_i^* - \xi_i - \xi_i^*)$$  \hspace{1cm} (2)

Among them $a_i, a_i^* \geq 0, \gamma_i, \gamma_i^* \geq 0, i = 1, 2, ..., k$, the function L corresponds to $\omega, b, \xi^*, \xi^*$ to minimize, corresponds to $a_i, a_i^*, \gamma_i, \gamma_i^*$ to maximize namely:

$$\frac{\partial L}{\partial \omega} = 0, \quad \frac{\partial L}{\partial b} = 0, \quad \frac{\partial L}{\partial \xi_i} = 0, \quad \frac{\partial L}{\partial \xi_i^*} = 0$$  \hspace{1cm} (3)

Finally, you can get:

$$\sum_{i=1}^{k} (a_i - a_i^*) = 0$$

$$\omega = \sum_{i=1}^{k} (a_i - a_i^*) x_i$$  \hspace{1cm} (4)

$$C - a_i - \gamma_i = 0, \quad i = 1, 2, ..., k$$

$$C - a_i^* - \gamma_i^* = 0, \quad i = 1, 2, ..., k$$

The maximization function is:

$$w(a, a^*) = -\frac{1}{2} \sum_{i,j=1}^{k} (a_i - a_i^*)(a_j - a_j^*)(x_i \cdot x_j)$$

$$+ \sum_{i=1}^{k} (a_i - a_i^*) y_i - \sum_{i=1}^{k} (a_i + a_i^*) \varepsilon$$  \hspace{1cm} (5)
Among them, \( \omega = \sum_{i=1}^{k} (a_i - a_i^*) x_i, 0 \leq a_i, a_i^* \leq C, i = 1, 2, ..., k \). The principle is similar to linear support vector regression, in which the optimization function is:

\[
w(a, a^*) = \frac{1}{2} \sum_{i,j=1}^{k} (a_i - a_i^*)(a_j - a_j^*)x_i \cdot x_j + \sum_{i=1}^{k} (a_i - a_i^*)y_i - \sum_{i=1}^{k} (a_i + a_i^*)e
\]

(6)

The constraints are: \( \omega = \sum_{i=1}^{k} (a_i - a_i^*) \varphi(x_i) \) and \( 0 \leq a_i, a_i^* \leq C, i = 1, 2, ..., k \).

3.2. Intelligent processing of network data

In the era of big data, informatization and intelligence have become the mainstream trends in the development of various industries. At the same time, computer network technology has been widely used. As a result, a large amount of network data information was born. How to effectively store, process, use and manage this information has become an important issue in the application of computer network technology. Artificial intelligence can effectively solve this problem. It has the dual functions of the human brain and the computer. It can store massive data information and analyse it effectively to select available, accurate, and high-quality information for the industry. Enterprise development provides strong information support and at the same time enhances the level of intelligence of computer network technology.

3.3. Reduce data processing and management costs

Using traditional network technology to process and manage data, human factors have a strong influence on its effectiveness. Whether it is data entry, verification or update, it needs people to complete, it is difficult to ensure the accuracy of data and management effect. Not only is it time-consuming and labour-intensive, it also causes a waste of resources and increases expenditure costs. Artificial intelligence can automate the entire process of data processing and management, automatically enter, check, and update data to avoid the influence of human factors, thereby ensuring the accuracy of data and management effects, further reducing corresponding costs, and creating a good development for computer network technology condition.

4. Cyber risk classification

4.1. Virus

Computer viruses are the most common and currently the most important security threat. With the development of computer network technology, computer virus technology is also rapidly developing and changing, and to some extent is ahead of computer network security technology. At present, computer viruses have developed to be no longer a simple virus, but include a variety of Internet-based network threats that endanger viruses, hackers, Trojan horses, spyware and so on. At present, the types of computer viruses are constantly changing, new virus variants are emerging one after another, and the destructive power tends to increase continuously.

4.2. Trojan

The Trojan ("Trojan Horse") program is actually a remote-control program, also known as a spy program, or backdoor program. As can be seen from the name of its "spyware", its main purpose is to engage in various espionage activities and collect user information; and from the name of its "backdoor", it can be seen that its successful intrusion is through the user's computer A program vulnerability in the system was carried out. Trojan horse programs are usually implanted in the user system through the remote UDP network communication process, and then use the C / S working mode to collect information, record user activities, view user passwords, modify user registry and
other illegal activities. At present, the threat of Trojan horses is increasing, and there are more and more Trojan horse programs. Moreover, the killing of such Trojan horse programs is much more difficult than the killing of computer viruses. Many professional computer virus protection programs are not very effective. Trojan killing program [3].

4.3. Network monitoring
Network monitoring is the network communication monitoring activities carried out by those who intend to invade and attack on the target network. Through network monitoring, you can obtain the required user information from the network communication flow, such as user account, password, IP address, MAC address, and also analyse the user's daily network activities and habits.

In the network, when the information is propagated, you can use the tool to set the network interface to the monitoring mode to intercept or capture the information that is propagating in the network. Network monitoring can be implemented at any location in the network. Hackers generally intercept user passwords through network monitoring. When they successfully invade a host, if they want to extend the results to the entire local area network where the host is located, monitoring is often the shortcut they choose.

4.4. Hacker attack
Hacking methods can be divided into non-destructive attacks and destructive attacks. Non-destructive attacks are generally for disrupting the operation of the system, and do not steal system information. They usually use denial of service attacks or information bombs; destructive attacks are aimed at intruding into other people's computer systems, stealing confidential information of the system, and destroying the data of the target system [6]. The methods of hacking are various and the harm is very great. At present, the methods and tools used by most middle-level and junior hackers still have many common features. They can be summarized as: network packet sniffing, IP address spoofing, password attack, denial of service attack and application layer attack.

5. Computer network security protection technology

5.1. Firewall technology
Firewall technology is currently a security technology that has a very important impact on computer network security, which can prevent the computer network system from being adversely affected and avoid the emergence of security problems. With the update of firewall technology, the significance of protecting computer network security has been redefined, making firewall technology more and more widely used. The firewall technology can not only protect the external communication network and avoid the entry of bad information, but also filter the internal network, making people's network environment more secure. Firewall technology has become an important part of protecting network security. With firewall technology, only communication content that meets security standards can be passed, which further improves the security of the network and avoids the invasion of intruders, as shown in Figure 3.
The advantage of firewall technology is that it can filter information through a filter to avoid the intrusion of harmful information, so as to protect the safe operation of the network and increase the speed of the network. It is a very efficient security technology. At the same time, when filtering data packets, it is completely transparent to the user. However, I have to admit that even the best technology is not perfect, and firewall technology still has certain flaws. If the firewall cannot completely prevent network spoofing, the security policy of the packet filtering firewall technology may also be abnormally executed, and the ability to resist hacker attacks is not strong, resulting in a malfunction of the computer network.

5.2. Encryption technology
For the security problem of computer networks, the application of encryption technology is becoming more and more extensive. After encryption, information will be more secure, which not only prevents information and data from being stolen by criminals, but also protects the network system from external attacks the security of the entire network. At the same time, people can also strengthen the protection of the information they need to protect through the key management system, so that the important information of computer users is more systematically encrypted to ensure their security and avoid external attacks. Using this encryption technology, you will not be distressed by the loss of information when transferring files. The transmission process is also encrypted to ensure that all data is safe enough during transmission to avoid loss [4].

5.3. Access control technology
Computer networks can not only share resources, but also spread viruses. Some websites are insecure. There are viruses such as Trojan horses. Once entered, they will be attacked by Trojan horse viruses, causing the entire computer system to malfunction. Therefore, access control technology is particularly important. It can strictly control people's access to the network, avoid entering harmful websites, and improve computer security. For example, the security of the network local area network can be achieved by controlling the router to ensure the stable operation of the computer system.

5.4. Vulnerability scanning and repair technology
System vulnerabilities will pose a threat to the security of the entire computer. If it is very dangerous, the system should be scanned for vulnerabilities in a timely manner to determine whether the vulnerabilities exist, and the computer system should be fully scanned regularly.
to ensure that there are no problems. Once a loophole occurs, the loophole should be repaired in time to avoid damage to the computer system in the long term.

5.5. Backup and mirroring technology
In order to ensure the information security of the computer network, it is necessary to back up the stored information, and the management personnel must also take appropriate protective measures, so that if there is an error in the system, there is no need to worry about data loss. You can also apply mirroring technology to start immediately when an error occurs to ensure the normal operation of the computer system.

6. Network risk prevention system design
In this paper, a network security information evaluation system is designed and implemented, and the GABP neural network model is applied to the system evaluation. At the same time, an evaluation demonstration is conducted by building a network to be evaluated. The network topology diagram is shown in Figure 4.

![Network Topology Diagram](image)

**Figure 4.** Topological structure diagram of computer network risk prevention and control system

The specific contents of the network security evaluation are mainly evaluated on five aspects: network topology topics, network structural elements, overall network comprehensiveness, network reinforcement schemes, and network situation. The focus of the evaluation in this paper is mainly on the evaluation and prediction of network structural elements and the comprehensive evaluation and prediction of overall network security.

The evaluation and prediction of network structural elements are divided into three different types. Different types of network topologies have different emphasis. The overall focus of the network to be evaluated adopted in this paper is mainly on the evaluation of the confidentiality of the network structure. The situation assessment diagram of the confidentiality of the network topology is shown in Figure 5. The figure mainly records the security trend of the network topology from December 10, 2017 to December 14, 2017 in detail. It also predicted the security situation of the system on December 15, 2017. It is not difficult to see from the trend diagram of the trend value that the trend value of the network topology structure shows a continuous downward trend [5].
7. Conclusion

In summary, artificial intelligence has the functions of efficiently processing fuzzy information, intelligently processing network data, reducing data processing and management costs, and has a positive effect on the development of computer network technology. In the context of the era of big data, artificial intelligence is supported by technologies such as big data and cloud computing, and can be applied to many aspects of computer network technology, such as network system management and evaluation, network security management and control, network agent management and network operation and maintenance. Wait. In this regard, we must fully explore the advantages of artificial intelligence, effectively apply it to computer networks, and promote the development of social information and intelligence.

References

[1] Sha, K., Alatrash, N., & Wang, Z. A secure and efficient framework to read isolated smart grid devices. IEEE Transactions on Smart Grid, 8(6) (2016) 1-13.

[2] Wu, Y., Cai, L., & Yang, H. A case study on environment risk assessment methods of coastal petrochemical project. Communications in Computer & Information Science, 482(2) (2015) 350-360.

[3] Pappas, Y., Jitka Veteková, Poduval, S., Tseng, P. C., & Car, J. Computer-assisted versus oral-and-written history taking for the prevention and management of cardiovascular disease: a systematic review of the literature. Acta medica (Hradec Králové) / Universitas Carolina, Facultas Medica Hradec Králové, 60(3) (2017) 97-107.

[4] Bahbah, E., Abdalla, A., Abdelshafy, K., Almohandes, A., Menshawy, A., & Aziz, M. E., et al. Should olanzapine be advocated over conventional anti-emetics for the prevention of chemotherapy-induced nausea and vomiting? An updated meta-analysis of randomized control trials. Current Enzyme Inhibition, 15(2) (2019) 80-90.

[5] Mckinstry, L. A., Zerbe, A., Hanscom, B., Farrior, J., Kurth, A. E., & Stanton, J., et al. A randomized-controlled trial of computer-based prevention counseling for hiv-positive persons (hptn 065). Journal of Aids & Clinical Research, 08(07) (2017) 85-92.