HILL PUBLISHING

Advances in Computer and Communications, 2023, 4(3), 181-185
https://www.hillpublisher.com/journals/acc/
ISSN Online: 2767-2875

Construction of Computer Network Security System in the Era of Big Data

Ying Lin

Northern Arizona University, Flagstaff, Arizona, USA.

How to cite this paper: Ying Lin. (2023) Construction of Computer Network Security System in the Era of Big Data. *Advances in Computer and Communication*, 4(3), 181-185.
DOI: 10.26855/acc.2023.06.015

Received: May 30, 2023
Accepted: June 28, 2023
Published: July 24, 2023

***Corresponding author:** Ying Lin, Northern Arizona University, Flagstaff, Arizona, USA.

Abstract

Computer network security is one of the important factors affecting the development of computer technology. Analyzing and exploring computer network security in the era of big data is conducive to achieving effective protection of data information. In the era of big data, there are many problems in China's computer network security system, such as information leakage and data tampering. Therefore, it is necessary to analyze the construction of computer network security system in the context of the big data era, clarify the construction ideas of computer network security system in the big data era, and build a comprehensive computer network security system based on this. With the continuous development and progress of science and technology in our country, we have entered the era of big data. In this context, big data technology is widely applied in various fields. However, at the same time, there have also been some problems, such as data leakage and tampering, which have had a negative impact on the application of big data technology. Therefore, it is necessary to strengthen research on the construction of computer network security system in the context of the big data era. Only in this way can we effectively solve the computer network security issues in the context of China's big data era. The era of big data is an era based on the Internet, with information data as the main resource and content. In the context of the big data era, China's social and economic development has been rapid, which has also driven the development of various industries. Internet technology has been widely applied in various industries. In the context of the big data era, people can obtain various information and knowledge through the internet. For example, a large amount of latest information about a certain industry or field can be retrieved through the internet; Communicate and communicate with others through the internet; You can purchase goods, book services, and more through the internet.

Keywords

Era of big data, computer network security, security system, key technologies

With the advent of the era of big data, computer network security issues have become increasingly prominent. Network security is one of the most prominent issues in the current development of the Internet, which not only causes economic losses but also poses a threat to national security. In order to ensure the security of the network system, a comprehensive security system is needed to protect the network system. This article will explore the construction of computer network security system in the era of big data, including the demands and challenges of network security, the composition of network security system, and key technologies. This article provides some ideas and methods with reference and guidance value for ensuring network security.

1. Demands and Challenges of Network Security

1.1 Basic Concepts of Network Security

Network security refers to the protection of information and communication systems in a network environment from unauthorized access, use, disclosure, disruption, modification, or destruction. Network security is essential for protecting the confidentiality, integrity, and availability of information and communication systems.

1.2 Analysis of Demands and Challenges

With the rapid development of information technology, the demands for network security are becoming increasingly diversified and complex. The following are the main demands and challenges of network security: Confidentiality: The confidentiality of information is the most basic requirement of network security. In order to ensure the confidentiality of information, it is necessary to prevent unauthorized access to sensitive information. Integrity: The integrity of information refers to the accuracy, completeness, and consistency of information. In order to ensure the integrity of information, it is necessary to prevent unauthorized modification or destruction of information. Availability: The availability of information refers to the ability of authorized users to access information. In order to ensure the availability of information, it is necessary to prevent unauthorized denial of service attacks. Compliance: Compliance refers to the adherence to laws, regulations, and industry standards. In order to ensure compliance, it is necessary to implement appropriate security policies and procedures. Risk Management: Risk management refers to the identification, assessment, and mitigation of risks. In order to ensure effective risk management, it is necessary to implement appropriate security controls and measures. Emerging Threats: With the advancement of technology, emerging threats such as advanced persistent threats (APTs), ransom ware, and zero-day attacks are becoming more common. These threats are difficult to detect and mitigate, which poses a significant challenge to network security.

2. Composition of Network Security System and Key Technologies

2.1 Basic Components of Network Security System

The composition of a network security system can be divided into three components: prevention, detection, and response. Prevention: Prevention refers to the measures taken to prevent security incidents from occurring. The prevention component includes access control, authentication, encryption, and firewalls. Detection: Detection refers to the measures taken to detect security incidents that have occurred or are occurring. The detection component includes intrusion detection systems (IDS), security information and event management (SIEM) systems, and vulnerability scanners. Response: Response refers to the measures taken to respond to security incidents. The response component includes incident response plans, disaster recovery plans, and business continuity plans.

2.2 Security Protection Technology

Security protection technology includes access control, authentication, encryption, and firewalls. Access control: Access control refers to the process of controlling who can access what resources in a network environment. Access control can be implemented through various methods such as role-based access control (RBAC) and attribute-based access control (ABAC).Authentication: Authentication refers to the process of verifying the identity of a user or device. Authentication can be achieved through various methods such as passwords, smart cards, biometrics, and multi-factor authentication.

Encryption: Encryption refers to the process of converting plain text into cipher text to protect the confidentiality of information. Encryption can be implemented through various algorithms such as Advanced Encryption Standard (AES) and RSA. Firewalls: Firewalls are network security devices that monitor and control network traffic based on predefined security rules. Firewalls can be implemented in various forms such as hardware and software firewalls.

2.3 Security Monitoring Technology

Security monitoring technology includes intrusion detection systems (IDS), security information and event management (SIEM) systems, and vulnerability scanners. Intrusion detection systems (IDS): IDS is a security technology that monitors network traffic for signs of security threats or attacks. IDS can be implemented in various forms such as network-based IDS and host-based IDS. Security information and event management (SIEM) systems: SIEM systems collect and analyze security-related data from various sources to identify and respond to security incidents. SIEM systems can be used for log management, event correlation, and threat detection. Vulnerability scanners:

Vulnerability scanners are tools that scan network systems for vulnerabilities and security weaknesses. Vulnerability scanners can be used to identify potential security risks and provide recommendations for mitigating them.

2.4 Security Emergency Response Technology

Security emergency response technology includes incident response plans, disaster recovery plans, and business continuity plans. Incident response plans: Incident response plans are pre-defined plans that outline the steps to be taken in the event of a security incident. These plans include procedures for identifying, containing, and mitigating the incident. Disaster recovery plans: Disaster recovery plans are pre-defined plans that outline the steps to be taken in the event of a disaster or major disruption to the network system. These plans include procedures for restoring the network system to its normal state as quickly as possible. Business continuity plans: Business continuity plans are pre-defined plans that outline the steps to be taken to ensure the continuity of business operations in the event of a major disruption to the network system. These plans include procedures for maintaining critical business functions and services. Summary and Future Outlook in order to ensure the security of the network system in the era of big data, a comprehensive security system is needed to protect the network system. This article has explored the demands and challenges of network security, the composition of network security system, and key technologies. The security system includes prevention, detection, and response components, with security protection technology, security monitoring technology, and security emergency response technology as the key technologies. In the future, with the continuous development of technology, the challenges of network security will become increasingly complex, and new security threats will emerge. Therefore, it is necessary to continuously improve and update the network security system to meet the new challenges and threats.

2.5 The Importance and Implementation Steps of Security Emergency Response Technology

The occurrence of cyber security incidents can cause irreversible damage to organizations and enterprises in terms of operations and reputation. Therefore, the implementation of security emergency response technology is one of the important measures to ensure network security. Security emergency response technology covers various aspects, including incident response, emergency response planning, and emergency response drills. Taking timely and effective measures during a security incident can minimize the impact on organizations and enterprises, while the development and execution of emergency response plans and drills can enhance their emergency response capabilities, allowing them to respond to security incidents more quickly and effectively.

The implementation steps for security emergency response technology can be divided into several aspects. First, it is necessary to develop an emergency response plan, clarifying the emergency response process and division of responsibilities, so that organizations and enterprises can respond quickly and effectively to security incidents. Second, it is necessary to establish a security incident response team responsible for analyzing and handling security incidents. Team members should have professional skills and knowledge to identify and respond to security incidents quickly and accurately. Third, it is important to establish a security incident monitoring and reporting mechanism to detect and report security incidents promptly. Fourth, emergency response drills should be conducted to test the effectiveness and feasibility of emergency response plans and processes, identify and solve problems, and improve emergency response capabilities. Finally, emergency response technology should be continuously improved and optimized based on emergency response plans and drill results.

In summary, security emergency response technology is one of the important measures for organizations and enterprises to ensure network security. By developing and implementing emergency response plans, establishing security incident response teams, establishing security incident monitoring and reporting mechanisms, and conducting emergency response drills, organizations and enterprises can enhance their ability to respond to security incidents and reduce the impact of incidents on their operations and reputations. In the face of evolving cyber security threats and attacks, security emergency response technology not only needs to respond to security incidents efficiently and promptly but also needs to be continuously improved and optimized to adapt to future challenges in network security [1].

3. Construction and Outlook of Network Security System

3.1 Basic Principles for Building Network Security System

Network security is an important issue in the information age, and the construction and development of the network security system requires adherence to certain basic principles to ensure the security and reliability of the net-

work system. The most important principle is comprehensiveness, which requires comprehensive security protection at all levels and stages, covering network hardware, operating systems, application software, data, and other aspects of security protection. This principle is the foundation for ensuring network security, as only comprehensive coverage can effectively prevent network security threats and attacks. Network security protection needs to be carried out according to different layers of security protection. This principle establishes the framework for network security protection, dividing network security protection into different layers, including network architecture, network transmission, application layer, and other aspects of security protection. This layered approach can more effectively prevent network security attacks and threats. Network security protection needs to consider practical applications and cost factors. This principle closely integrates network security protection with practical applications, considering both security and usability and economic feasibility. Network security protection must meet the requirements of practical applications and should not be too complex or cumbersome, while also considering cost issues and avoiding excessive expenses. Network security protection needs to be flexible in responding to different security threats and attacks. This principle establishes the flexibility and adaptability of network security protection, as network security threats and attacks are constantly changing, and network security protection needs to be flexible in responding and adjusting security strategies and measures at any time to ensure the security and reliability of the network system. Network security protection needs to have sustainability to ensure the long-term safe operation of the network system. This principle closely integrates network security protection with the long-term operation and development of the network system, ensuring the security and reliability of the network system. Network security protection needs to be constantly updated and upgraded to cope with the constantly changing network security threats and attacks, while also considering the long-term development and operation of the network system to ensure its stability and sustainability [2].

3.2 Practical Suggestions for Building Network Security System in the Era of Big Data

In the era of big data, network security faces greater challenges and demands, and the construction of the network security system also needs to adopt some practical suggestions to ensure the security and reliability of the network system. Firstly, it is necessary to strengthen network security awareness education. Although technology is constantly improving, users' security awareness and prevention capabilities are still the first line of defense for network security. Therefore, it is necessary to popularize network security knowledge and skills to users through various means, to improve their awareness and prevention capabilities. Secondly, it is necessary to strengthen research and development and application of network security technology. With the arrival of the era of big data, network security faces more complex and severe challenges, and traditional security technologies are no longer able to meet practical needs. It is necessary to continuously explore new network security technologies, such as artificial intelligence, blockchain, etc., to improve network security protection levels. These new technologies also need to be applied to practical network security protection, continuously improving the application scenarios and effectiveness of network security technology. Thirdly, it is necessary to strengthen network security monitoring and early warning. Network security threats and attacks are constantly changing, so it is necessary to strengthen network security monitoring and early warning to detect and deal with network security problems in a timely manner. By establishing an efficient monitoring and early warning mechanism, network security threats and attacks can be quickly detected and responded to, ensuring the security and reliability of the network system. Fourthly, it is necessary to strengthen network security management. Network security management is an important means to ensure the security of the network system, and it is necessary to establish a sound network security management system, including security policies, security regulations, security procedures, etc. By strengthening network security management, network security problems can be effectively prevented and controlled, ensuring the long-term safe operation of the network system [3].

3.3 Future Outlook of Network Security System in the Era of Big Data

In the future, with the constant development and application of big data technology, the network security system will also face new challenges and opportunities. Looking ahead, the network security system will pay more attention to data security and privacy protection, strengthening security protection for emerging technologies such as artificial intelligence and the Internet of Things. At the same time, network security technology will become more intelligent, automatically identifying and responding to network security threats through machine learning and automation technology. In addition, the network security system will gradually extend to the cloud and edge, strengthening security protection for new network architectures such as cloud computing and edge computing. Cross-border coop-

eration and open sharing will also become an important trend for the future network security system, as different countries and regions will strengthen cooperation to jointly address network security challenges and promote the sustainable development of network security.

4. Conclusion

In summary, network security is an important issue in the information age and a necessary condition for ensuring the security, reliability, and stable operation of the network system. The construction and development of the network security system require the comprehensive use of various technical means, the establishment of a sound security management system, the improvement of users' security awareness and prevention capabilities, and the strengthening of international cooperation and open sharing to jointly address network security challenges and promote the sustainable development of network security. In the future, network security will face more complex and severe challenges, and it is necessary to continuously promote technological innovation and management innovation, optimize the network security system, and better ensure the security and reliability of the network system, as well as promote the development of information construction and socio-economic development.

References

[1] Chen, Z., Wang, S., & Xiang, H. (2018). A review of network security risk assessment methods. Journal of Electronics & Information Technology, 40(3), 501-509.

[2] Xu, J., Liu, H., & Xie, Y. (2020). A review of network security in the era of big data. Journal of Big Data, 7(1), 17.

[3] Wang, W., Zhang, Y., Li, C., & Zhang, Z. (2019). Network security protection technology based on machine learning. Journal of Physics: Conference Series, 1251(1), 012019.

[4] M Xiao, M Guo. (2020). Computer network security and preventive measures in the age of big data. Procedia Computer Science, 2020.

[5] Y Tang, M Elhoseny. Computer network security evaluation simulation model based on neural network. Journal of Intelligent & Fuzzy Systems, 2019.