Research on Optimization Strategies of Computer Network Security Technology in the Era of Big Data

Qiyi Liang, Yuqing Gong
School of Computer Science, Zhuhai College of Science and Technology, Zhuhai, China

Abstract: With the continuous development of information technology, the challenges faced by computer network security also show a significant upward trend. How to protect computer network security more effectively, it is necessary to comprehensively analyze the current situation of computer network security under the background of big data, and formulate targeted optimization strategies to provide protection for computer network security. Based on the current situation of computer network security under the background of big data era, this paper analyzes the optimization strategy.

Keywords: Era of Big Data; Computer; Network Security Technology; Strategy

1. Introduction

In the context of big data, the problems and challenges faced by computer network security have a significant increase. As the amount of data continues to increase, the complexity of the network topology continues to increase, and potential network vulnerabilities also have a significant increase, which affects data security and may even cause data leakage[1]. According to the conventional computer network security technology, the management of computer security has been unable to fully meet the needs of computer network security management under the background of big data. It is necessary to focus on the current situation of computer network security under the background of big data era to improve the management measures.

2. Current Situation of Computer Network Security in the Era of Big Data

2.1 Large-Scale Data

In the context of big data, the amount of data collected and stored by various facilities is increasing at an extremely fast rate. Unilaterally relying on traditional network security technology for security management has been unable to cope with the challenges brought by massive data in the context of big data[2]. In the process of network security management, it is more necessary to adopt more accurate and efficient technology to dynamically monitor all kinds of data, find potential security risks in time, and deal with them in time.

2.2 Diversified Network Attack Methods

In the context of the era of big data, there are obvious diversified characteristics of network attacks, which will directly affect computer network security. There is a continuous evolution and upgrading of the methods and means of network attacks, which leads to a significant increase in the incidence of computer network security vulnerabilities[3]. At the same time, some traditional network attacks, including phishing, malicious code, etc., have not completely disappeared, and are also hidden in the network to pose a threat to network security. With the continuous development of information technology, some new types of attacks are frequent. By using artificial intelligence attacks, zero-day vulnerability exploitation, etc., it is easy to pose a greater threat to computer network security.

2.3 High Difficulty in Privacy Protection

In the era of big data, the difficulty of protecting data information has further increased. The protection of corporate trade secrets and personal privacy information is an important part of computer network security management. With the continuous development of modern information technology, the use of various intelligent mobile terminals may involve a large amount of identity information, financial data and other content[4]. Once information leakage occurs, it may affect personal privacy and property. In the process of enterprise information management, frequent enterprise information leakage will exert adverse effects on the development and interests of enterprises themselves. Against the background of big data,

the scale and quantity of data processing have increased significantly, and traditional privacy protection measures can no longer fully meet the growing demand for security information.

3. Optimization Strategies of Computer Network Security Technology in the Era of Big Data

3.1 Continuous Improvement of Big Data Security Risk Prediction Technology

In the context of big data, to effectively enhance computer network security and respond to various security risks and threats, it is necessary to continuously improve big data security risk prediction technology, predict potential security risks of network technology, and guarantee the security of computer data information. Based on large-scale data analysis, big data security risk prediction technology analyzes massive data through machine learning and deep learning models to assess whether abnormal behaviors exist. Through risk prediction, abnormal data can be accurately identified and risk early warnings can be issued to predict potential network attacks[5]. Meanwhile, in the context of big data, security risk prediction technology can achieve continuous learning and adaptation, and constantly optimize and adjust the prediction model to cope with more complex network attacks. According to the application of the currently deployed big data security risk prediction technology, this technology can analyze network traffic, system logs, user behaviors and other content to form a more comprehensive network security awareness system, thereby accurately predicting network risks. It should be noted that with the continuous development of information technology, network risk prediction technology also needs continuous optimization and upgrading to further enhance its role in computer network security management.

3.2 Rational Application of Information Encryption Technology

Using information encryption technology to protect computer network information is an important measure to safeguard network data security. Encrypting various types of data with security keys ensures that even if the data is intercepted by external parties during transmission and storage, the content of the data cannot be obtained. In the context of big data, information encryption technology has been gradually applied to data management in government, medical, financial and other industries. The use of information encryption technology can effectively guarantee the security of data transmission and protect user privacy to avoid the risk of information leakage[6]. At present, there are many types of information encryption technologies, including symmetric encryption technology, encrypted data storage, asymmetric encryption, security protocols and so on. Although such technologies are relatively mature, based on the diversity and complexity of computer network security protection, it is necessary to continuously improve information encryption technology with the continuous development of information technology, so that this technology can serve computer network security more accurately and efficiently.

3.3 Improvement of Users' Information Security Awareness

In the context of big data, to more effectively protect computer network information security, it is necessary to continuously enhance users' information security awareness. Users should have good risk identification capabilities in daily use of computer network systems and accurately judge potential security problems in the network system. When logging into the network system, users should attach importance to the protection of accounts and passwords and try to avoid logging into accounts in insecure environments. Before logging in, users should accurately analyze the security and reliability of websites to prevent random access to unqualified websites that may lead to personal information leakage. Meanwhile, users should give priority to logging in through official platforms instead of third-party platforms when logging into accounts[7]. Users are not allowed to click on pop-ups and other links in websites at will to avoid personal information leakage. When setting login passwords, users can appropriately increase the complexity of passwords on the basis of easy memorization by using a combination of letters, numbers, symbols and other characters. In addition, passwords can be designed by combining static passwords with dynamic biometric passwords to improve password security.

3.4 Continuous Optimization of the Data Recovery System

Computer virus intrusion will affect the automatic operation of programs and may cause partial data loss or automatic data deletion, thus affecting data security. To ensure the security of network data information, it is necessary to continuously improve and upgrade the data recovery system and perform proper data backup. Meanwhile, backup data and original data should be stored in different storage units as much as possible to ensure data security. Even after virus intrusion, various types of data can be backed up in a short time through the data recovery system, thus ensuring data security. Especially for enterprise users or financial industry users, in the process of network data security management, it is necessary to accurately apply the data recovery system for data management and regularly maintain and upgrade the data recovery system.

3.5 Strengthening Data Security Management

In the context of big data, data exchange is the most important content in the operation of computer networks. How to manage security during data exchange plays a vital role in ensuring data security. There are many channels for computer network data exchange with a large volume of data exchange. Once a security hazard occurs in a certain data exchange link, it may threaten data security. To ensure the security of network data information, attention should be paid to data security management and the level of data management should be continuously improved. Firstly, it is necessary to refine management during data collection to guarantee data security from the source. Make full use of all kinds of anti-virus software or technology to evaluate the security of data, to avoid some viruses or Trojans hidden in the data, after entering the system to other data threats, and even cause information leakage. At the same time, it is necessary to restrict the standardization of data exchange operations. The management personnel responsible for data entry need to operate in strict accordance with the prescribed process in the process of data exchange, so as to avoid the impact of non-standard operation on data security.

3.6 Create an Active Defense System based on Artificial Intelligence Technology

In the traditional operation mode, network security defense is mostly a passive response problem, that is, to carry out corresponding detection and disposal after being attacked, which has the defects of lagging response and low processing efficiency. In the big data environment, artificial intelligence technology should be actively used to create an active defense system, and real-time modeling and anomaly detection of network behavior should be realized through deep learning, reinforcement learning and other algorithms. The information system automatically learns massive historical data, and the artificial intelligence model can confirm normal behavior patterns. When abnormal behaviors that deviate from normal patterns are found, early warning will be automatically issued or corresponding blocking measures will be taken. For example, the anomaly detection technology based on generative adversarial networks has high accuracy in detecting unknown types of network attacks, which can obviously make up for the shortcomings of traditional signature library dependence. At the same time, the adaptive learning ability should be integrated into the active defense system, pay close attention to the changes of network environment attack means, and constantly update the parameters of artificial intelligence model according to the latest changes, so as to ensure that the detection accuracy is always at a high level and reduce the false alarm rate.

3.7 Establish A Zero-Trust Security Architecture

In the era of rapid development of big data, the network boundary is gradually blurred. Traditional boundary defense models such as firewalls and VPNs are difficult to cope with advanced persistent attacks on the network in the new era, and it is difficult to identify and deal with internal threats. The key to the zero-trust security architecture is 'never trust, always verify'.Users use the internal network or external network to access, and each access request must complete the steps of identity authentication, permission verification and behavior audit. In the process of designing a zero-trust security architecture, the network can be divided into logical units of different granularity by using micro-isolation technology, and the communication between each logical unit must be authorized separately. At the same time, the software defined boundary technology is used scientifically to hide the network service port before the user and the device have completed

the verification, so that the attacker can not find the potential target. Finally, the implementation of the zero-trust architecture also needs to combine dynamic behavior analysis, access control and other measures to ensure the minimum access to data resources and achieve full-link protection of big data.

3.8 Enhanced Data Desensitization and Privacy Computing Technology

In the era of big data, data analysis and mining work usually need to be analyzed based on the original data. There is some sensitive information in the original data. If sensitive information is directly exposed in the network environment, privacy leakage may occur. Data desensitization technology can transform sensitive fields on the basis of retaining statistical characteristics of data, or directly replace sensitive fragments with other words, so that data users cannot be directly related to specific individuals or entities. The commonly used data desensitization methods include masking, substitution, perturbation, generalization, etc. Privacy computing refers to allowing multiple users to perform joint computing without sharing raw data with each other. The privacy computing path includes secure multi-party computing, federated learning, trusted execution environment, etc. For example, the federated learning technology path allows each data user to train the model in the original storage path, only upload the model parameters in the network system, and the original data is retained in the original storage path, so as to effectively protect the privacy of data users. Financial institutions and medical institutions can scientifically apply data desensitization and privacy computing technology to effectively avoid data leakage while giving full play to the value of data.

4. Conclusion

Computer network security is a concern of the current society. Ensuring network information security plays an important role in ensuring the normal advancement and development of all aspects of things. However, according to the actual situation, the challenges faced by computer network security in the context of big data have a significant increase, which will pose a threat to network security. It is necessary to accurately analyze the potential problems in the process of computer network security management based on the characteristics of the era of big data, and timely formulate management measures in all aspects, optimize management technology, and provide guarantee for computer network security.

References

[1] Huang Lan. Thoughts on the Optimization of Computer Network Security Technology in the Era of Big Data[J]. Information Recording Materials, 2025, 26(06): 239-241.

[2] Zhang Chengting, Cheng Chao, Ye Wanxing, et al. Application Strategies of Computer Network Security Technology in the Era of Big Data[J]. Computer Knowledge and Technology, 2025, 21(06): 86-87+96.

[3] Zhu Hao. Analysis on Information Security Issues of Computer Network Technology and Its Prevention Strategies in the Era of Big Data[J]. Information Recording Materials, 2024, 25(09): 43-45.

[4] Zeng Haifeng. Optimization Strategies of Computer Network Security Technology in the Era of Big Data[J]. Cyberspace Security, 2024, 15(04): 232-235.

[5] You Xiaoge. Optimization Strategies of Computer Network Security Technology in the Era of Big Data[J]. Digital Technology and Application, 2024, 42(08): 78-80.

[6] Ma Xiumei. Optimization Strategies of Computer Network Security Technology in the Era of Big Data[J]. Digital Communication World, 2024(06): 201-203+206.

[7] Ye Dong. Optimization Strategies of Computer Network Security Technology in the Era of Big Data[J]. Network Security and Informatization, 2024(04): 124-126.

