

Research on Big Data and Computer Information Security Technology Based on Data Cube

Ying Zhou, Pancheng Li

Jiangxi Police institute, Nanchang, 300003, China

Keywords: Big data; Computer network; Security Technology

Abstract: The emergence of big data era provides a basis for the vigorous development of computer network technology. With the popularization of Internet technology, computer information network brings opportunities for social progress and the development of the industry, but at the same time, there are also many problems. With the continuous improvement of information technology in China, information security is facing great challenges. It is particularly important to constantly innovate and improve computer information security technology. This makes network security in a big data environment an important research topic, involving technology, management and usage. Based on this, firstly, the related overview of computer network security is expounded. Secondly, the hidden dangers of computer network security in the era of big data are analyzed. The technology of computer network security maintenance is expounded again. Finally, the full text is summarized.

1. Introduction

With the application of modern information technology in the computer network, the emergence of big data technology has been promoted, and the modern network structure has been changed. It is necessary to establish a safe and effective network information technology security protection system in order to effectively manage the network big data [1]. As we all know, the network has a strong virtuality. Netizens communicate and communicate in the virtual space, to a certain extent, it will contribute to the possibility of cybercrime. At the same time that big data brings great convenience to the world, network security issues are also becoming more and more obvious. As the amount of data becomes doubled, the types of data are more complicated and diverse, and network viruses and networks The technology of hackers is also constantly developing [2]. If we can't handle the big network security problem well, it will have a big negative impact on our big data era, and it will directly affect people's use efficiency and effect on massive data information.

The wide application and rapid development of computer network technology has spawned the emergence of big data. The development and convenience of computer technology has made computer technology occupy a place in all walks of life and play an increasingly important role [3]. However, computer network technology has great security risks in the application process. Once a problem occurs, it will bring huge economic losses to individuals and even enterprises. Therefore, it is imperative to strengthen the security protection of computer information. The computer realizes resource sharing and information transmission through computer network, which promotes information dissemination. However, in the process of its development, network information will also be damaged, tampered with, malicious dissemination and other incidents, improving computer security processing technology is a powerful guarantee for information sharing [4]. In order to effectively guarantee the security of massive information in the network, it is necessary to analyze the security technology of big data and cloud computing, explore the information security guarantee system of big data under the network environment, and promote the development of network information security management technology.

2. Overview of Computer Network Security

For the background of big data era, computer network security related overview mainly from the

integrity of the system, security, confidentiality and other three aspects of analysis. Since the emergence of the network, hackers have been born. It can be said that hackers are the undesirable products of the development of network information. As the core of data processing and operation, many users' files are stored and processed in the third-party platform, which also contains some sensitive information. Its security and privacy are being challenged greatly [5]. The application of big data is very extensive and involves many fields, such as the application in enterprises, which can make the management of enterprises more efficient and reduce work pressure. The user login authentication, that is, the secure login authentication technology, is used in the computer network to verify and authenticate the correctness of the data source and the integrity of the information. It is mainly used for resource access between operating systems. From the perspective of confidentiality, computer network is an important medium for information exchange. Ensuring the security and confidentiality of information is an important part of computer network security maintenance [6]. Once the computer system itself has a loophole, there will be errors in the software, and the system is vulnerable. It is the most serious security risk of all the vulnerabilities. These vulnerabilities create opportunities for hackers and viruses to invade, especially the vulnerabilities of enterprise computer systems. Will bring huge property losses to the company.

3. Analysis of Computer Network Security Hidden Danger in Big Data Era

3.1 Network hackers

The spread of network viruses is manipulated by hackers. Hackers appear with the emergence of the network. They are the products of information networks. Some hackers attack computers not for economic benefit, but to meet their own needs. Hackers appear to meet their own hobbies. With the advancement of network technology, the threshold for hackers is getting lower and lower. A large number of hackers are constantly appearing in big data environments, which poses a serious threat to network security. Hackers attack information systems, causing information leakage or information systems to be completely paralyzed, which has a great impact on users' use.

3.2 computer virus

With the continuous development of Internet technology and new technologies, anti-virus software is constantly updated. Similarly, network viruses are constantly improving and constantly overcoming the security barriers of anti-virus software. Computer viruses refer to programs with wake-up breaks for computer operating systems. These programs include spy viruses, Trojan horse viruses, script viruses, etc. Some users do not check for foreign media in order to export data faster, or the computer system cannot play the role of killing. The Trojan virus attacks the user's computer system and downloads the personal information in the system. The spy virus uses the web link to attack the user's computer system and steal key data without the user's knowledge or unawareness. The spy virus mainly attacks the user's computer through the linked web page, and steals the user's personal data without the user's knowledge.

3.3 Operating System Security Hidden Danger

Computer system vulnerabilities will cause computer software errors, any program and system have vulnerabilities, but the system vulnerabilities for users' network information is a major security risk. At the same time, there are unpredictable security risks. To ensure the information security of Internet protocols, a computer toolbox should be established, but many users are not aware of this problem. Some users have a weak sense of security in the process of using computer networks. In the process of logging in to some websites, they leak their personal information, and often do not conduct virus killing or browsing records processing, etc. Continued dissemination provides convenience. After a problem with the operating system itself, there will be problems with the user data management of the system. Frequently repairing the operating system can effectively reduce the damage caused by system vulnerabilities.

3.4 Ck of safety awareness among operators

In the era of big data, we should enhance the security awareness of every netizen. For enterprises, we should train employees' safety awareness, which can effectively reduce the possibility of unnecessary risks caused by staff operation errors. In the big data environment, user privacy data greatly increases the risk of leakage. If the user improperly uses the private data and the data is related, it will have more serious consequences. In the process of running a computer system, it is necessary to ensure that all applications of the computer can be used normally. Computer core technology and many computer operation technologies have powerful management functions, which can manage the operation status of computer software and hardware infrastructure and equipment. The network provides a variety of channels for netizens. Netizens can get the resources they want more conveniently through the network, but sometimes users inadvertently open a website or a link will paralyse the computer network.

4. Application of Network Security Technology Based on Network Security Maintenance

4.1 Wall Technology

As the main barrier of computer network security, firewall is currently the most widely used defense technology in the world. Basically every computer will set up a network firewall. The working principle of firewall is to monitor the computer all-weather at the source of computer work, effectively cut off the access of computer viruses to computer systems, and fundamentally reduce the harm of viruses to computer systems. In the context of big data, computer information presents a diversified trend. Combined with the Internet protocol of IP, computer information systems can realize the sharing and processing of information resources safely and effectively. The firewall is applied in multiple environments of the Internet, indicating that the firewall plays an important role in information security protection. The firewall can ensure the security and stability of the network information, which is an inevitable need to ensure computer information security. The various firewall pairs of the computer are shown in Table 1.

Table 1 Computer various firewall comparison

Classification	Characteristics
Simple packet filtering firewall	Application layer control is weak and efficient
Stateful inspection packet filtering firewall	Packet filtering is transparent to users and efficient
Application proxy firewall	Application layer control is weak and detection performance is high

4.2 S detection and killing technology

In the era of big data, the update speed of viruses is more rapid. Therefore, during the application of these anti-virus software, users must update the virus database regularly to effectively protect the mainstream viruses on the market. Currently, the more popular computer virus killing software on the market has 360 protection, King soft Internet Security and so on. These software can detect the vast majority of computer network viruses, which need to update the virus database regularly. Computer network viruses are ubiquitous. Therefore, it is necessary to strengthen the prevention of computer network viruses and regularly detect and kill computer systems, so as to ensure the security of computer networks and improve the security level of users.

4.3 SS Rights and Data Encryption Technology

The principle of access rights technology is to control the operator's access to the network. The operator's access to some websites requires the user's access authorization. This technology can effectively control the computer's access to viruses. After setting up network access rights, if operators want to access some websites or some computers or some software systems, they need administrator's authorization for their accounts. Otherwise, they will not have access rights. This

defense method can effectively control the probability of computer-virus contact. Applying intrusion technology to computer systems can effectively improve the security of computer information. Monitoring technology enables effective monitoring and supervision of the environment in which the computer operates. This measure can improve the security of information and ensure that information is not destroyed. Through the encryption of the double-ended line, it ensures that the information is stable and reliable in the process of transmission, and the dynamic conversion of plaintext and cipher text greatly increases the difficulty of cracking, and plays an important role in information protection. In order to ensure that the published data information will not reveal confidentiality, it can also ensure the traceability of data leakage, and can effectively deal with the security problems that occur during the release of big data.

4.4 Usion Detection Technology

Intrusion detection technology is a computer software that collects information about applications and data packets, and finds possible intrusion behaviors from the information. When a certain high probability of intrusion occurs, the software will automatically alarm. This requires data mining technology to process data. Big data mining security refers to ensuring the security of mining data in the process of processing massive amounts of information. The behavior of intrusion may be mined from the massive information. Once it is judged that there is a high probability of intrusion in the system, the software will automatically alarm and cut off the channels of hacker attacks and virus intrusion in time to ensure the network information of the computer. Safety. In addition, we can also use encryption measures to properly separate the data use process from the data storage process, and to protect the key in the data management cycle. To establish a sound computer information security protection mechanism, enterprises need to integrate a large number of data and information, conduct accurate investigation of security issues, so as to improve the perfection of enterprise computer information security organization. With this system, we can effectively resist the entry of illegal viruses. This detection system will become a powerful assistant of firewall security system and anti-virus software. It can pre-judge and deal with any attack on computer information network in advance through professional analysis methods.

5. Conclusion

In summary, the network is a double-edged sword. In the era of information network, the technology of information network transmission has indeed brought a lot of convenience to our life, but the security of computer network has become an important factor affecting the development of information network technology. Therefore, major enterprises should constantly improve information security management measures, regularly use anti-virus software, strengthen the use of intrusion technology and monitoring technology, install firewalls and so on, so as to effectively guarantee the security of enterprise internal computer information system. Based on the perspective of big data, this paper conducts in-depth research on network security technologies in the era of big data. After research, readers can understand the concept and characteristics of big data, and on the basis of understanding the concept of network security, understand that in the context of big data, network security risks mainly come from network hackers, viruses and operating systems themselves. In order to improve the information security processing technology in the era of big data, it is necessary to transform the computer network into a cloud computer network, and realize the transformation of the computer network by separating the data from the hardware. However, this technology also requires relevant personnel to jointly study.

Acknowledgement

The project was funded by the 2015 Jiangxi Provincial Economic Crime Investigation and Prevention Technology Collaborative Innovation Center and Jiangxi Electronic Data Forensic Key Laboratory.

References

- [1] Yadav G, Dalal S. Improvisation of Network Security using Encryption Technique for Big Data Technology [J]. International Journal of Computer Applications, 2015, 124(11):27-30.
- [2] Zhou L. Big Data Based on Fuzzy Grey Information System Security Intrusion Detection Research [J]. Advanced Materials Research, 2014, 1079-1080:4.
- [3] Rathore M M, Ahmad A, Paul A, et al. Urban Planning and Building Smart Cities based on the Internet of Things using Big Data Analytics[J]. Computer Networks, 2016, 101(C):63-80.
- [4] Siddiqa A, Hashem I A T, Yaqoob I, et al. A Survey of Big Data Management: Taxonomy and State-of-the-Art[J]. Journal of Network and Computer Applications, 2016, 71:151-166.
- [5] Nie S H. Analysis of Computer Information Processing Technology in Era of Big Data[J]. Applied Mechanics and Materials, 2014, 687-691:2772-2775.
- [6] Chen Z, Wen Y, Cao J, et al. A survey of bitmap index compression algorithms for Big Data[J]. Tsinghua Science and Technology, 2015, 20(1):100-115.