Research on Computer Network Information, Network Security and Protection Strategies Based on Big Data Mining

Qiang Mei

Jiangxi University of Engineering, Xinyu, Jiangxin 338000 China

Keywords: Big Data Mining: Computer Network Information, Network Security, Strategy

Abstract: under the Background of Continuous Social and Economic Development, Information Technology Has Ushered in a Peak Period of Vigorous Development. At This Stage, with the Development of Information Technology, the Era of Big Data Has Come, Which Has Changed the Means of Obtaining Data and Information in the Past, and Computers Are Facing Some Network Security Problems. under This Background, the New Generation of Computer Information Engineering Technology Will Get Great Development, and Information Technology Represented by Computer Technology is Also Changing People's Production and Life Style. in the Environment of Big Data Mining, People's Demand for the Mining and Utilization of Big Data Mining Has Become Increasingly Strong, Which Also Makes Computers the Main Tools for People to Mine and Utilize Data. This Paper Analyzes and Narrates Big Data Mining to Some Extent, and At the Same Time Puts Forward Relevant Policies for the Current Situation of Computer Network Security in the Era of Big Data for Reference.

1. Introduction

In Recent Years, the Popularization and Application of Computers in Various Fields Have Brought Far-Reaching Impacts on People's Production and Life Styles and Greatly Promoted the Development of Various Fields [1]. under the Environment of Big Data Mining, Computers Have Created Extremely Favorable Development Conditions for the Application of Big Data Mining Technology and Improved the Application Level of Data in Various Fields. the So-Called Big Data Mining Mainly Refers to the Establishment of a Big Data Mining Platform to Obtain Relevant Information Data and Process Them to Establish a Database So That People Can Select and Search the Required Data According to Their Actual Needs through the Computer Terminal [2]. in the Era of Big Data, the Problem of How to Prevent Information Leakage in the Use of Computer Networks Has Become a Very Important Topic. Computer Network is Closely Related to People's Life. Cloud Computing's Super-Strong Data Processing Capability and Large Amount of Data Collection, Application and Sharing Not Only Meet the Real-Time Demand, But Also Push Computer Network Security to the Forefront Again, Becoming a New Challenge Direction for Information Security in the New Era [3]. the Criminal Activities Generated by the Computer Network Have Also Increased Greatly. Computer Network Security Can Not Only Deeply Affect the National Security and Social Security, But Also Directly Affect the Personal Security of the Public. Therefore, the Research on the Prevention of Information Security is Urgent.

Big Data is Defined as: “Big Data Technology Describes a New Generation of Technology and Architecture, Which Extracts the Economic Value of Various Large Amounts of Data through High-Speed Collection, Discovery or Analysis.” through This Definition, the Characteristics of Big Data Can Be Summarized into 4 V, Namely Volume, Variety, Velocity and Value, as Shown in Figure 1.

DOI: 10.25236/ISMHI.2019.113

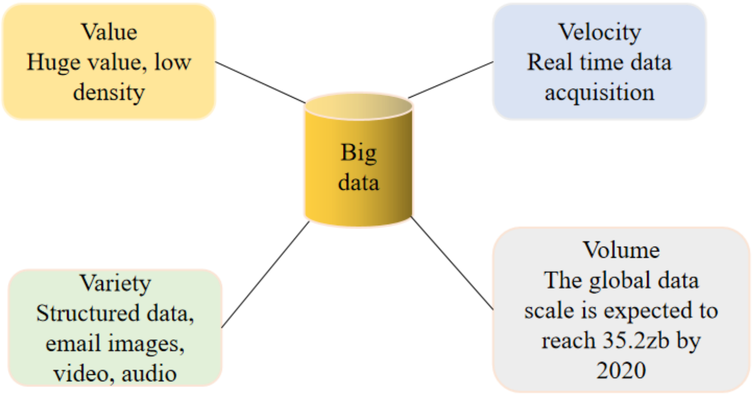
Value
Huge value, low density
Velocity
Real time data acquisition
Big data
Variety
Structured data, email images, video, audio
Volume
The global data scale is expected to reach 35.2zb by 2020

Fig.1 The 4v Characteristics of Big Data

2. Importance of Maintaining Computer Network Security in Big Data Era

2.1 The Accuracy of the Data Can Be Improved

Maintaining computer network security in the era of big data can improve the accuracy of data to a certain extent. Data collection and collation in the era of big data have corresponding characteristics, mainly including large data acquisition range, diverse data processing methods and large data storage space. The strategic significance of big data mining technology lies not in mastering huge data information, but in specialized processing of these meaningful data [4]. In other words, if big data mining is compared to an industry, then the key to the profitability of this industry. On the one hand, the Internet gives us great freedom. Anyone can speak freely in the Internet age and spread to any corner of the world, full of free will. On the other hand, the progress of digital technology also brings the possibility of tracking all information, which is completely transparent to the network. According to the above characteristics, we can know that the digital information in the era of big data is very complex. To build a strong database, we must first ensure the accuracy of the data. At present, besides relying on the computing power of the data platform, we must also attach importance to the maintenance of computer network security and reduce the processing difficulty of information data from the root [5]. Big data mining technology has improved its processing ability while changing its data processing methods. At the same time, it has also made a new change in processing methods. It has effectively improved the value of data. It can be said that this is the place where big data mining can be commended.

2.2 The Service Quality of the Big Data Mining Platform Can Be Strengthened

Maintaining computer network security in the era of big data can also enhance the service quality of big data mining platforms. To build a complete data platform requires a series of complicated steps, and the data platform is equivalent to a huge storage [6]. Big data mining cannot be processed by a single computer, and a distributed architecture must be adopted. Its characteristic lies in the distributed data mining of massive data. But it must rely on cloud computing distributed processing, distributed database and cloud storage, virtualization technology. Big data mining is based on a public platform. Behind the location and behavior analysis, people's data information still faces huge risks of being traded and stolen, while cloud services aggravate the risk of information disclosure [7]. Users can retrieve information and data through selection and search, which reflects the service of the data platform. Nowadays, more and more users will choose to acquire information through the data platform, which will provide storage, calculation and other functions according to users' needs. In other words, if a computer is infected by a virus, other parts of the computer system will also be attacked by the virus. Computer viruses can cause damage to the normal operation of the computer and endanger the data information inside the computer. If the virus is serious, it will also cause the computer system to crash.

2.3 Is Conducive to the Integration of Big Data Mining Resources

Maintaining computer network security in the era of big data can integrate data resources more effectively. In the era of big data, people are constantly creating new data resources when using and sharing information and data resources. Based on the increasingly close connection of data, the design and implementation of the interconnection of all things will affect the whole body. Once a certain link is breached and big data mining is polluted and tampered with, the whole data chain will be attacked, causing immeasurable heavy losses [8]. If the network security supervision is not in place, the consequences will be that important information will be lost or damaged by criminals. What's more, important information will be stolen directly and used for illegal activities, which will seriously interfere with the social security and is not conducive to the stability and harmony of the country. People can acquire data through computer networks or upload data through computer networks. In the process of resource interaction, there must be a corresponding computer network security protection system to protect network security [9]. The advent of the big data era has brought a brand-new expansion space for computer network technology. It has added more color to people's life, but it has also strengthened the virus infection ability virtually, thus bringing bad influence to the computer operation environment. Therefore, it is necessary to update the security testing software frequently, master the relevant strategies to prevent computer viruses, and use the security testing methods after fully understanding computer viruses to effectively prevent computer viruses.

3. Security Problems of Computer Network in Big Data Era

3.1 External Security Problems of Computer Networks

The external security problem of the computer network is mainly a kind of security problem that exists in all computer networks. It is not caused by the security vulnerabilities of the computer network itself, but will occur whenever and wherever people use the computer network [10]. As we all know, when computer users shop and socialize online through the network, merchants often analyze users' network behaviors by collecting traces and privacy information browsed by users in the network, so as to adopt accurate marketing and achieve the purpose of increasing product sales. Moreover, from the current situation, a considerable part of the network security awareness is relatively weak, and the management of personal information is not very strict. This has created a great potential safety hazard for personal information. For example, when we register and log in to a website, our IP address may be virtually collected and collated by the name of the website. Big data mining contains huge information, and the privacy of computer information cannot be guaranteed. Security defense tools commonly used in computer work are difficult to distinguish hacker attacks. If the computer is attacked by hackers, the losses caused will be difficult to recover.

3.2 Internal Security of Computer Network

The internal security problems of the computer network mainly lie in some security vulnerabilities of the computer network itself. The computer network is not a single one. It is composed of numerous servers. There is a certain complexity when the computer network is set up. If we don't pay attention to solve the internal security risks existing in the computer network itself, corresponding problems will arise. For example, when a computer user makes a purchase or registers an account on the network, the login password set is too simple, the user does not think his information will be stolen, and holds great fluky psychology, which will inevitably bring great economic and reputation losses to the user once his personal information is stolen. In particular, some government departments, universities and other organizations have their own local area networks, which record a large amount of data and information. If there is no corresponding security awareness, once the information is leaked, the consequences will be unimaginable. For example, in the process of data transmission using computer networks, sudden network interruption or network delay will cause network vulnerabilities in a short period of time, giving criminals an opportunity. The full popularity of mobile devices attracts the dark forces of the network to shift more targets to mobile terminals, which will continue to increase the difficulty of security protection for big data mining storage systems.

3.3 Viral Security Problems in Computer Networks

Viral security problems of computer networks are common at present, and they are also a kind of computer network security problems with comprehensive public awareness. In addition, there are many computer users who have not repaired the network vulnerabilities in time. The version of anti-virus software used is too old and they do not pay attention to security when downloading software. This makes criminals often use these vulnerabilities to attack users' computers and steal users' important personal data and privacy information. Because once a link goes wrong and discloses the user's information, the information will be used by some criminals. At this stage, although some anti-virus software has appeared on the market, these anti-virus software can only deal with general computer viruses. For some viruses with strong attack, these anti-virus software still appear a little chicken ribs. At present, the most harmful virus existing in computer networks is aggressive virus. Aggressive virus is mainly a kind of computer network virus with strong pertinence. It can accurately destroy the computer network in a certain area and spread through the network. Generally, it is difficult to clean up this virus. In essence, Big Data Mining is valuable information transmitted and accumulated by various nervous systems of the Internet cloud brain during operation, and is the basis for the cloud brain to generate intelligent intelligence. If machines have self-awareness and autonomous behaviors through the Internet of Things in the future, they will also pose new security threats to mankind.

4. Countermeasures to Improve Computer Network Security in Big Data Era

4.1 Innovative Use of Quantum Encryption Technology

In the era of big data, the most direct and effective way to better deal with computer network security problems and improve the level of computer network security protection is to explore innovative network security encryption technology. Only by comprehensively improving computer users' awareness of network security can hackers and criminals be ensured that there is no way to carry out network attacks. Therefore, strengthening computer users' awareness of network security is an important prerequisite and fundamental measure to ensure computer network security. For example, when users input personal information on the Internet, they should make the password as complex as possible so as not to allow illegal elements to take advantage of it, thus increasing the difficulty of deciphering the password and ensuring the safety of their own information.

Technical protection means refers to the encryption of important data. the encryption model of general technology is shown in Figure 2. its technical mechanism is as follows: encryption is performed according to the computer encryption algorithm, so that the generated code cannot be directly read. when extracting information, the password must be used for decryption.

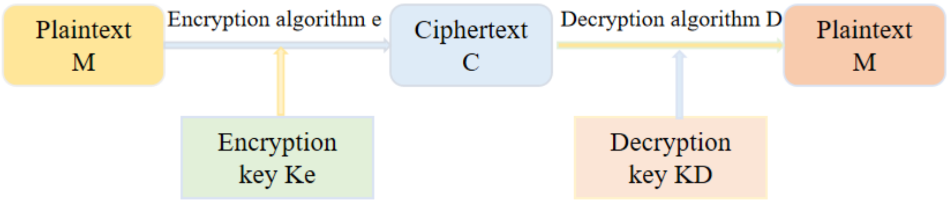

Fig.2 General Data Encryption Model

At present, quantum encryption technology is recognized by scientists as the most effective method to ensure computer network security. However, since quantum encryption technology is still in the research stage, its popularization and application may take a long time. The computer firewall is taken as the first barrier to prevent illegal invasion, and cloud computing is used to further optimize and upgrade the technology and add intelligent identification function. Different networks are divided into different security levels, and the firewall intelligently identifies which networks are accessible and which networks are threatened.

4.2 Enhance Hierarchical Protection of Computer Networks

At present, the most important measure applied to computer network security protection is firewall technology. However, with the advent of the big data era, the sharing of information and data resources is increasingly prominent. In order to continuously improve the size of firewall technology, it is necessary to strengthen the hierarchical protection of computer network. China should fully learn from the legislative experience of other developed countries in computer network security, and combine with the actual situation of our country to establish a legal system of computer network security protection that conforms to our characteristics, clarify the responsibilities of computer network security protection, and strengthen the supervision of computer network security incidents. Therefore, in addition to strengthening the safety awareness of users, the anti-virus ability of computers should also be improved. It is best to establish a relatively perfect virus defense system to reduce the invasion of external viruses on computers. There is a certain level difference between computer networks. Computer networks can be distinguished according to different purposes and different functions, and corresponding firewalls can be set up between area networks with different purposes. Using encryption technology, the information transmission in the era of big data is processed by multiple encryption methods, such as key encryption technology and remote access control. Each step combines authentication with password encryption to ensure that the main contents of the data will not be stolen or truncated in case of any security threat during transmission.

4.3 Strengthen the Detection Technology of Computer Virus

At present, our country already has relatively mature computer virus detection technology. On this basis, we should further strengthen the prevention and removal functions of virus detection technology. For the same kind of data, its encryption method is also different. On the basis of ensuring the safety of big data mining storage space, the data should be prevented from being stolen by hackers or criminals to the greatest extent during transmission. Even if hackers or criminals steal the data, they cannot crack the contents of the data. In addition, the security protection of sensitive data has become the top priority of big data mining application security. At the same time, the operating environment of big data mining involves various levels of network, host, application, computing resources, storage resources and so on, which requires in-depth security protection measures. Using big data mining statistical analysis, anomaly detection is carried out for users' non-habitual operations. If there is illegal invasion, defense measures are taken immediately to deal with it. Secondly, aiming at the existing intrusion behavior, the virus and intrusion data resource database is established, and real-time monitoring and comparison analysis are carried out to further strengthen the protection capability. In the process of users using computers, early warning is given to the links that may be infected with viruses, and some less destructive viruses can be removed autonomously, while still ensuring the safety in the process of using computer networks.

5. Conclusion

The management of data information security includes network management, data management, equipment management, personnel management, etc. It is a system engineering, so we need to rely on a complete data and information security management system. In the era of big data, it is very urgent to solve the problem of computer network security. In order to make a big leap in computer network technology, we must do a good job in the corresponding security protection and make a comprehensive analysis of computer network security. We should not only attach great importance to network security and continuously improve the research and development of security technologies, but also spare no effort to improve users' security awareness and strengthen the normative cooperation between the government and the international community. Computer network security cannot be achieved overnight. It requires our joint efforts to achieve it.

References

[1] Shi K. (2017). Research on the Network Information Security Evaluation Model and Algorithm Based on Grey Relational Clustering Analysis[J]. Journal of Computational & Theoretical Nanoscience, 14, no. 1, pp. 69-73.

[2] Pak W, Choi Y J. (2017). High Performance and High Scalable Packet Classification Algorithm for Network Security Systems[J]. IEEE Transactions on Dependable & Secure Computing, 14, no. 1, pp. 37-49.

[3] Jia J, Tang S, Xie H, et al. (2017). Mobile Visual Search: a Survey[J]. Jisuanji Fuzhu Sheji Yu Tuxingxue Xuebao/Journal of Computer-Aided Design and Computer Graphics, 29, no. 6, pp. 1007-1021.

[4] Yu Y, Au M H, Ateniese G, et al. (2017). Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage[J]. IEEE Transactions on Information Forensics and Security, 12, no. 4, pp. 767-778.

[5] Li T. (2017). Analysis of Computer Network Information Based on "Big Data"[J]. IOP Conference Series Earth and Environmental Science, 94, no. 1, pp. 012195.

[6] Cui L, Tso F P, Pezaros D P, et al. (2017). PLAN: Joint Policy- and Network-Aware VM Management for Cloud Data Centers[J]. IEEE Transactions on Parallel & Distributed Systems, 28, no. 4, pp. 1163-1175.

[7] Alkasassbeh M. (2017). An empirical evaluation for the intrusion detection features based on machine learning and feature selection methods[J]. Journal of Theoretical & Applied Information Technology, 95, no. 22, pp. 5962-5976.

[8] Chembe C, Noor R M, Ahmedy I, et al. (2017). Spectrum sensing in cognitive vehicular network[J]. Computer Communications, 97, pp. 15-30.

[9] Praude C C. (2018). Computer Art and Actor-Network Theory: Actants and Intersubjective Associations in Scene[J]. Leonardo, 51, no. 5, pp. 529-529.

[10] Song Z, Xingjian W, Wei L. (2017). Survey of network security situation awareness[J]. Electronic Test, 269, pp. 3281-3286.