Information Data Security in the Era of Big Data

ELEC5032M Modern Industry Practice

Spring 2020

Abstract

With the rapid development of the Internet, big data has become the trend of the times. Internet technology has also been widely used in all sectors of society. However, the following information security problems have also caused problems for related technical personnel. How to maintain network security under the guidance of big data has become a hot topic in the society. This article first introduces big data, then outlines the current status of network security and analyzes its problems, finally proposes ways to strengthen information data security.

Introduction

Big data refers to a technology that can quickly and efficiently obtain useful information from mass information [1]. The current big data has the following characteristics: huge amount of data, diverse types of data and fast processing speed [1]. The huge amount of data is a basic characteristic of big data. With the improvement of technology, people's requirements for data are gradually approaching the thing itself. The data that needs to be processed also increases exponentially, so that the technology could be more accurate. The variety of data means that there are more and more current communication methods, including video, pictures, audio, and so on. Furthermore, it is no longer limited to unified structured data. There are other types of data, which also increases the difficulty of processing. The feature of processing data very fast is well supported by people. Sending and receiving messages to others in time, which makes the information exchange between people faster and convenient.

Current status of information data security

• Disregard of information confidentiality

With the advent of smart phones, it has entered every aspect of people's lives and individuals cannot leave it at most times. People use smart phones to record life, shop online, pay, etc. These methods can easily leak information. It is possible to attach your personal information or family information to a website or application, which may be exploited by some persons or companies to leak personal privacy.

• Defects in technology

Nowadays, the security of the Internet is threatened by many factors, including viruses, hackers, etc. have caused many enterprises and companies to suffer losses. Hackers are a group keen on innovative attack technologies. Their technology is very powerful and can destroy other people's computers to obtain information and data for profit. Therefore, more professional network security technicians are needed to improve the security level.

• Business Negligence on Information Security

There are some companies don't distinguish between secret-related equipment and ordinary equipment as well as between secret-related personnel and ordinary personnel [2]. In other cases, in the current network environment, managers of computer information in enterprises must pay special attention to the operating environment of computers and guard against danger [2]. In today's enterprises, there is a phenomenon when computers are running, a virus intrusion was discovered. However, the computer's managers do not maintain the system in all directions, but simply carry out a virus check and kill. It causes the possibility of hacker invasion, causing serious users information leakage.

• Impact of malware

Malware is not uncommon in the application market. Unscrupulous merchants entice users to download and install malware. It steals user information, monitoring user operation information, and forcing advertisements, etc., which has extremely impaired user information security Great harm [3]. Due to the high concealment and complexity of malicious software, it is difficult for people to find these malicious applications. Even if security protection software is installed, some malicious applications can bypass scanning and detection. This is also the reason why mobile Internet security issues are serious today.

Methods to strengthen information and data security

• Legal protection of information and data

The use of data is wide and it has penetrated almost every aspect of life. The current big data is intimate and intelligent, which can allow people to pay attention to social

dynamics and things related to people themselves. For example, individual can use the medical website to check physical or mental health through big data technology. From a macro perspective, it is necessary to establish related laws to strengthen information and data security. Legal formulation departments can issue some normative documents, so that the security issue is no longer limited to professional fields. For instance, European Union published The long-awaited General Data Protection Regulation (GDPR) on May 25, 2018, which is powerful for the data privacy and cyber security [4].

• Supervision

In the era of highly developed Internet, the accuracy of data is higher, so the value it brings is naturally greater. In order to make high profits with small cost, some organizations will choose to steal user information for illegal purposes. For such a situation, government can set up a supervision department that is responsible for examining whether the running code contains viruses. After all, humans and machines are also different. Humans can handle all kinds of unexpected situations, but machines could not. In this way, the security of information and data can be more guaranteed.

• The application of security technology

The country should vigorously support the development of the information industry as well as the education in information technology. At the same time, continuing to cultivate talented competitive talents is also necessary. For relevant technical departments, they must also fully understand their own shortcomings. It is essential to find possible weak links in code and programs, select them for special research and work out the perfect protection scheme [5]. They can also abstract models for existing problems and design specialized protection tools. It will play a warning role to continuously improve the technical level and security performance of hardware firewalls. In these ways, network attacks and virus transmission can be detected in a timely manner.

Conclusion

In the era of big data, more and more information is collected and applied, which means information security is particularly important. In the current situation facing many risk situations, traditional protective models have become inadequate. People

must continue to develop stronger methods. I believe that in the future, a scientific and convenient system will be used and people's information security problems will be better solved.

Reference:

[1] Dong, Xin Luna., and Divesh. Srivastava. *Big Data Integration* First edition. San Rafael, California (1537 Fourth Street, San Rafael, CA 94901 USA): Morgan & Claypool, 2015.

[2] Wang, Haijun. “Research on Network Information Security Model and System Construction.” SHS Web of Conferences, vol. 25, EDP Sciences, Jan. 2016, doi:10.1051/shsconf/20162502010.

[3] Zhang Maoyue. *New threats and protection of personal information and data security in the era of big data* [J]. China Science and Technology Forum, 2015 (07): 117-122.

[4] Kalman, Laurence. “New European Data Privacy and Cyber Security Laws - One Year Later.(General Data Protection Regulation, Network and Information Security Directive)(Hot Topics / Europe Region: GDPR).” Communications of the ACM, vol. 62, no. 4, Association for Computing Machinery, Inc., Apr. 2019, pp. 38–38, doi:10.1145/3310326.

[5]“Intelligent Information Network Security and Management.” China Communications 13, no. 7 (July 2016): iii–vi.