Network Security in the Era of Big Data

Zhong Feiyu
School of Information and Telecommunication Engineering, Beijing University of Posts and Telecommunications, 100876, China

Abstract. The convergence of three networks and the increasing progress of storage technique have ushered in the era of big data. As big data has key economic and political values, network security under the background of big data has become the focus of attention. Improving these network information security issues requires the joint efforts of the state, enterprises and individuals. The state needs to improve the definition of sensitive information, regulate the behavior of enterprises and individuals, and each user raises the awareness of network security prevention. It is believed that with the progress of technologies such as data encryption and data storage, network security issues will be better resolved.

1. Introduction
At the same time, with the progress of the Internet and the Internet of Things, the Internet of Everything enables people to collect and store information such as network behaviors, preferences, and accumulated knowledge and experience in different fields, providing rich materials for the era of big data. With the progress of storage technique and the integration of the three networks, people's storage capacity for information has been greatly improved, providing technical support for the era of big data. We have entered the era of big data with massive data explosion. The development of data mining, semantic engine, visual analysis and other technologies makes it possible for us to analyze big data [1]. We can deeply analyze from the massive data. Through the analysis and calculation of the big data, we can get the analysis results based on the massive data.

Big data has the characteristics of huge amount of data, various types and high value. The analysis of big data has gradually formed a new generation of information processing methods. Compared with the traditional technique, big data can quickly, accurately and cheaply predict the future industry development and personal preference trend, which has a very important value in communication, search, customer analysis and other aspects [2]. Therefore, big data can bring huge commercial value and has become the focus of competition for every enterprise. In the military field, the advantages of situation control, intelligence analysis and joint operations can be brought into play in the battlefield through the analysis of a large number of data. At the same time, because of the wide source, mixed data and diverse formats [3], big data also contains the user's personal privacy information. If it is leaked, it will be easily controlled by criminals and cause damage to life and property, which will facilitate the implementation of criminal behavior. While enjoying the convenience of big data, we should also see the hidden dangers brought by big data. All in all, the network security defense under the background of the big data era should be paid attention to by people.

2. The Potential Harm of the Network under the Era of Big Data

2.1 Aggregate Storage of Big Data and Cross-Checking Lead to Information Leakage
In the era of big data, enterprises that do not analyze data will be thrown away by the wave of the
times. Enterprises that analyze user data can better grasp the business process under the guidance of this information, and do business direction for the enterprise. Make a wise choice. Therefore, most companies have collected, traded, and integrated big data driven by interests. The big data is partly derived from the sensors of mobile phones, computers and other devices and the analysis of people's life behaviors. Most of big data is unstructured data types. Although scalable, the storage model is not mature. When a large number of data such as cell phone sensor records, social network records, e-mail and chat content are gathered, and many data such as operation data and customer personal information of some companies are stored. Due to the unscientific and standardized management, the centralized storage method is adopted instead of sorting and classifying the data assets, which greatly increases the risk of information disclosure [4].

With the rapid development of big data in recent years, the sensitivity of whether information can be disclosed has not been specifically defined in law. In the process of data collection and exchange in the early stage of big data analysis [5]. Inevitably, there will be a small amount of information outflow. Due to the fuzzy definition of sensitivity, even if the information is not much, it may carry personal, enterprise and even national privacy information, but because of the wide source of big data. Cross-checking can confirm the user's real information and identity, which poses a great threat to network security. Among them, the medical and financial industry involves personal privacy and property information, and the data sharing with other industries is obvious, even small leaks can cause immeasurable risks.

2.2 There is a Problem with the Protection of Big Data Itself
In the era of big data, traditional hacking attacks still exist and still threaten. At the same time, new types of cyber attacks are gradually increasing, and the losses are increasing. Attackers' attacks are more inclined to use the platform for automated attacks, which is less noticeable and has specific goals, lurking for a long time to prepare for the attack. Once the hacker attack is successful, we can use big data to mine user information at the same time. With the increasing understanding of the user information, it can attack the user more pertinently, endanger the safety of the user's life and property, and further expand the danger caused by information leakage.

Cloud computing promotes the development of big data and provides a platform for big data, but at the same time it does not provide sufficient guarantee for the security of big data. For example, the application programming interface's access rights and key management are not standardized, which may lead to data leakage. In addition, big data itself can be used as a carrier for hacker attacks, and hackers can insert viruses that obtain information into big data. Big data itself is characterized by high value but low value density. Big data has various forms and complex structure. In this case, when enterprise cloud computing, data mining, machine learning and big data analysis are used to obtain information, these attacks hidden in big data will unconsciously attack and copy users' information [6].

Due to the huge content of big data, if normal data security scanning is adopted for these massive data, it will inevitably take a lot of time and be too inefficient. This shows that information security protection and retrieval methods have not been upgraded with the vigorous development of big data. Massive data brings great difficulties to security protection, and the security protection of big data faces some threats.

2.3 Information Security Problems Caused by Weak Network Security Awareness
with the progress of the Internet, mobile APP and WEB applications have become an indispensable part of people's lives. Each application requires users to register their accounts and fill in some user information. In the context of big data, this information has a certain degree of relevance. Some users are not aware of the network security awareness, leaking personal information on the social platform, leaking location information on the take-away and taxi software, and leaking personal property information on the wealth management software. Some users use the same password on each platform account and the password complexity is not high, and there is no habit of changing passwords regularly. These all increase the risk of disclosure of personal information. In addition, the user's rights
management for the application is not in place. Some application merchants are in need of information collection, and they want to understand user preferences to specifically market products. These applications use the trust of users. At the same time of providing services to users, we excessively ask for the privacy rights beyond the rights required to provide services, and use these rights to collect user information in the background. Even some enterprises, driven by huge interests in the era of big data, collect personal information of users and enterprises in the background, and even trade with third-party platforms. This kind of weak security awareness of users and information collection of businesses make it easier for attackers to steal information, thus causing threats to users' lives and properties. Smith et al. [7] pointed out that there are four data dimensions related to privacy disclosure in the process of data processing: information collection, misuse, secondary use and unauthorized access. All of these have greatly threatened the personal privacy security of users and the data security of enterprises.

3. The Solution of Big Data Network Security

3.1 Pay Attention to the Standardized Management of Big Data
The country needs to strengthen the propaganda of big data network security awareness and strengthen the training of big data network security talents. So as to promote the research and development of big data security technology, increase investment in the research and development of key technologies of big data security, and ensure that the development of network security technology can keep pace with the development of big data technology.

As a new developing technique, big data needs perfect policies to restrain the new problems brought by its industrial development. For example, the state should standardize the management of information security, have perfect restrictions on the sensitivity of user information, and have clear regulations on the punishment of malicious collection and data disclosure. The country needs to clarify the scope of big data in the secret field and develop a sound management system and operational guidelines. Severe punishment for violations of national cybersecurity. On the enterprise side, it is recommended to strengthen the introduction of relevant talents, standardize the internal data management of enterprises, especially regulate the use of mobile devices, and formulate effective solutions.

Enterprises and governments should take precautions against the security of data, make backup and restoration plans for data in advance, and formulate effective contingency plans after data loss. Use backup for restore as soon as possible after data loss to minimize the loss.

The process of big data security is mainly to standardize the construction. It is very important to form a set of orderly and sustainable development ecology, and a set of standardized operation mechanism, management system, construction and sharing standards. The processing of big data in a unified framework not only improves the data analysis speed, but also reduces the threat of data leakage. In addition, a set of supporting security systems should be generated to ensure the security of big data for the security center in the big data environment. Under the premise of vigorous development, it is even possible to establish an open data, secure and orderly big data sharing platform.

3.2 Improve User Information Security Awareness
As a user of privacy and application, the user's security awareness is an effective way to curb privacy leakage in the era of big data. First of all, we must form a sense of privacy, and do not use our own private information, especially on public networks and public social platforms. Secondly, for mobile phone and web application, we should have a certain degree of vigilance for access. The control of application access is an important measure to prevent information leakage and ensure network security.

Enhance the publicity of network security, and strengthen personal management of computer accounts, payment accounts, social accounts, etc. In daily life, we advocate that users should strengthen the awareness of network security, not expose their account and password at will, ensure the security of user information, pay attention to the complexity of password when setting the
password, and should not use the same password multiple times. Personal account information should not be stored under non-private network conditions and should be cancelled in time. Finally, it is necessary to periodically change the password according to actual needs, and regularly perform software updates and virus killing on the personal computer, which can also improve the risk prevention effect to a certain extent [8].

3.3 Perform Rights Management and Encryption of Data
First of all, strict access control is required for those who obtain data. The purpose of this measure is to conduct strict certification and hierarchical authority management for those who have access to the data. This is an effective means to prevent hackers from intruding. Other specific measures may be passwords, passwords, or other privileged symbols that are periodically replaced with access settings to assist authentication. It can also generate specific measures for each user to fundamentally control the path of hackers’ intrusion into the database and prevent the confusion of permissions. Setting permissions for network users is a good hierarchical management, which can flexibly control the information with different sensitivity, reduce the number of people who can access the more sensitive information, and effectively improve network security.

Data encryption is an important method to protect the safe operation of the network. Data encryption is the most reliable means for computer systems to protect information. Encryption algorithm can be quickly divided into symmetric encryption algorithm and asymmetric encryption algorithm. It uses cryptography to encrypt information, conceal information, and ensure that all sensitive information is stored in ciphertext, thus protecting the security of the content. It is based on the original rights management, and another protection measure for data, and can not protect the data from being leaked. In this case, even if the hacker gains access to the data by masquerading, it will be blocked in the encryption processing of the information.

4. Summary and Prospect
With the development of network technology, the development of computer storage technology, operation technology, cloud computing and data analysis, we have ushered in the era of big data. With the popularity of big data, its requirements for network security are getting higher and higher. Although big data plays an important role in people's daily life, enterprise management and national strategic development, the network security issues in the big data era have also received attention. Due to improper storage of big data, cross-validation of big data, vulnerability of big data itself and weak awareness of network security of users and enterprises, big data has great security risks. In order to solve these problems, the state needs to pay attention to the standardized management of big data, and strengthen the safety awareness of users and the safety of data encryption [9].

The security of big data requires not only technological innovation, but also the common writing of society, enterprises and users. With the advent of the big data era, network security management should keep pace with the times and continue to develop to ensure the safety of big data and the privacy of users, and ensure that big data can become a security ladder for social development.

References
[1] Guo Sanjiang, Guo Yanjin. Data security research in big data environment [J]. Science and technique Plaza, 2013 (2): 28-31
[2] Feng Wei. Information security opportunities and challenges in the era of big data [J]. China Science and technique investment, 2012 (34): 49-53
[3] Wang yuanzhuo, Jin Xiaolong, Cheng Xueqi. Network big data: current situation and prospect [D], 2013
[4] Feng Dengguo, Zhang Min, Li Hao. Big data security and privacy protection [D], 2014
[5] Liu Yahu, Zhang Tieying, Jin Xiaolong, et al. Personal privacy protection in the era of big data [J]. Computer research and development, 2014: 1
[6] Ding Jia. Network security research based on big data environment [J]. Network security technique
and application, 2014 (4): 116-116

[7] Smith H J, Milberg S J, Burke S J. Information privacy: measuring individuals' concerns about organizational practices[J]. MIS quarterly, 1996: 167-196.

[8] Zhao Jun. the importance of network security in the era of big data [J]. Digital technique and application, 2017 (1): 216-217

[9] Bansal G, Zahedi F. The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation[J]. ICIS 2008 Proceedings, 2008: 7.