Analysis of Information Security Risk Defense in the Development of Big Data

Yuexing He* and Jingzhou Ji
School of Information and Communication, National University of Defense Technology, Xi'an, Shanxi, China

*Corresponding author e-mail: 17391615859@sina.cn

Abstract. Big data plays an extremely important role in the development of social economy. The information security of big data is related to the security of people's personal data and important information of governments and enterprises. This article analyzes the concept of big data and the information security risks under the development of big data, And from the social, technical supervision and other aspects, Discussed information security risk defense methods under the development of big data.

Keywords: Big Data, Information Security, Risk Defense

1. Introduction
The rapid development of big data makes it extremely popular in various industries[1]. Greatly improve people's work efficiency and quality of life. Some existing big data risk assessment techniques based on grey theory, There is a certain guarantee for the security risk assessment of the big data database, Able to discover database security vulnerabilities in time, and establish a corresponding defense system, Improve the security of big data database. At present, a certain amount of attention is paid to the defense of big data security risks, and takes corresponding measures to maintain information security.

2. The Concept of Big Data
Big data is generally a large-scale data collection that cannot be crawled and processed in conventional ways[2]. The way of processing big data should use more discovering and efficient processes to process information materials with large orders of magnitude, rapid growth, and complicated styles. The importance of big data is mainly to analyze and mine data in a professional way, Discover the connection between information materials[3], And predict the future. The current widespread application of big data in education, business, science and other fields, Conducive to the rapid development of the economy and society.

Prevent and resolve information security risks in the development of big data, The global data space has no borders, Big data has become a weapon for games and contests between big countries. Strengthen information security in the development of big data, It is based on the identification of information security risks, Comprehensive policy, Prevent and resolve information security risks in the development of big data, Prevent information security incidents from occurring and reduce information security incidents.
incident losses. The closed loop of information security governance consisting of information security strategy and big data risk identification, prevention, resolution, and summary links is shown in Figure 1.

Fig.1 Information security management closed loop

3. Causes of Information Security Risks in the Development of Big Data

3.1. Virus Damage
During the operation of the big data network, One of the main factors that harm and affect its security is the big data virus. Once the virus invades the big data system, will cause some damage to it. And it is difficult to repair effectively[4]. And, The virus spreads relatively fast, It is difficult to effectively solve it. When the big data network information system suffers from a virus, It mainly exhibits three characteristics: First of all, is highly concealed, once the virus invades the big data successfully, will be activated immediately, there are also some viruses that will be latent after invading, then be activated at a specific time and operation, and was not discovered in time, lead the big data network in a dangerous state. Secondly, is highly destructive, after the virus invades big data, Will spread the entire big data system comprehensively, And cause some damage, Once the relevant file program is destroyed, it will make the system difficult to start and run normally. At last, Is highly infectious, The existence of big data virus, Ignore any restrictions, Direct infection of files in big data, Even if it is processed by killing software, It is difficult to guarantee complete removal, It can even cause files to be erased and destroyed, Then the virus will reproduce and infect itself in the big data network system, This leads to the generation of information security risks in the development of big data[5].

3.2. Trojan Horse Damage
Big data Trojans are also one of the main factors that lead to the destruction of big data network security performance, But it has something in common with the virus, More obvious in terms of concealment. At the same time there is a big difference, The virus mainly obtains personal benefits through extortion and extortion, The Trojan horse is to directly view the information in the big data system, Obtain important information such as personal property and information without the knowledge of others. Big data in the process of being compromised by Trojan horses, The main characteristics of its performance are also manifested in three aspects. First of all, Its operability is high, During the operation of the Trojan in the big data network, Intruders can control by contacting big data, Extract important information contained in big data. Secondly, Highly implantable, under normal circumstances, Trojans will be attached to files or corresponding program software, People operate by downloading, Activate it, And then through its higher spread, Embed the Trojan in the big data system[6]. At last, It has high stubbornness, Once the Trojan is carried out in the big data system, It will be difficult to remove, Lay hidden dangers for the information security of big data development.
3.3. Wrong Operation
From the perspective of the development status of the safe operation of big data network systems, human error operation is also an important factor leading to the destruction of its safety[7]. In the process of using big data network, most personnel cannot take corresponding preventive measures, cause some wrong operations, threat to the security of big data systems, these wrong operations are mainly manifested in three forms, one is that criminals used to imitate well-known websites, expand the visibility of the website, so as to steal information and related data of registered users. Second, many criminals registered a large number of mailboxes, distribute messages widely, if the person responds as required by the email, will cause personal information or related accounts to be leaked[8], the third is affected by the chaotic network environment, a large number of advertisements flood the website, it will lead to hidden Trojan horses in some ads, threat to the security of big data systems.

Secondly, users face new risks due to data hosting, as shown in Figure 2. Data concentration in the context of big data technology. Generally, user data is transferred to cloud computing service providers (data centers) for hosting to achieve centralized data storage. The new risks it faces include: Priority access risk, after the user hands over the data to the cloud computing service provider; Data location risk, when customers use cloud computing services, they don't know which server their data is stored on, I don't even know in which country this server is placed; Data isolation risk, a large amount of user data is almost in a shared environment in the cloud computing service platform and it is difficult to isolate; Data recovery risk, whether user data can be restored and how long it can be restored depends on the cloud computing service provider’s ability to back up and restore data, rather than the user; Long-term development risk, if the user chooses a cloud computing service provider, will always expect this service provider to develop steadily, continue to provide corresponding services, if cloud computing service providers disappear, it may bring "catastrophic" loss of data for users.

4. Information Security Risk Defense Methods for Big Data Development
4.1. Establish a Big Data Information Security Guarantee System
Information security protection should be carried out in the stages of data collection, processing and use, establish a big data information security guarantee system[9]. The scope of big data data collection includes sensor collection and network information data collection, leading to a wide range of big data collection sources. Data encryption and other technologies can ensure the security of data collection, use VPN virtual private network to establish data transmission path, use cloud storage and other technologies to improve the security of data storage, and under the premise of ensuring privacy, mining and analyzing big data, improve the security of data processing. Supervising big data security can improve the effectiveness of big data information security work. Use the authentication system to ensure
the control of data usage. Training and introducing information security technical personnel can also strengthen the defense of data and information security risks. Enabling technical experts to conduct a security risk assessment of the database, Predict the security trend of the database in advance.

4.2. Build a Hierarchical Management and Control System for Big Data and Important Data
In the information security risk defense of big data, based on the sensitivity and importance of big data, Establish a hierarchical control system, Differentiate management of data. The government’s information management and control should focus on the monitoring of key industries and sensitive data. Establish a management mechanism for sensitive databases. For the information management and control of the enterprise, attention should be paid to the supervision of sensitive information within the enterprise, Strengthen the management of personnel, facilities and corporate data, Avoid leakage of important enterprise data.

4.3. Improve Big Data Security Monitoring and Emergency Response Capabilities
Big data information security risk defense should establish a big data security supervision mechanism, Real-time monitoring of the operation of big data, And improve the emergency response capabilities of abnormal conditions. Establish a big data information security emergency response system, And cooperate with certain emergency agencies, Set up emergency response plan, When an information security incident occurs, Ensure that the emergency plan can be activated in time, And can handle the accident efficiently, It is also necessary for relevant work management staff to evaluate the effect of emergency response after the event. Combining analysis results to strengthen security risk defense measures, To protect the defense capabilities of big data information security.

4.4. Strengthen the Communication of Big Data Information Security Risks
The perception of information security risks of big data varies greatly among different stakeholders. Exchanges between stakeholders should be increased, Improve people's understanding of information security risks. At present, some people have limited understanding of big data information security issues. Need to strengthen information security education and publicity work, Enable experts in related security fields to communicate with the public, To avoid the spread of misleading information security knowledge. It should also increase the development of information security risk defense technologies and products, Use advanced technology to establish a universal security defense system for network users, Incorporate big data information security risk defense into public affairs. Enterprises and the public should pay attention to the communication with the trustee when carrying out data storage and mining. Jointly control security risks.

Fig.3 Information security management system framework based on data
5. Conclusion
My country’s big data technology is still in the development and construction stage, Network security issues are constantly updated and complicated, Attention should be paid to information security risk prevention work, Guarantee people's normal production activities. The defense of big data information security risks, Information security should be integrated into the social level. Use relevant laws and information security assurance agencies to strengthen the supervision of big data information, Improve the exchange of security risk issues between various stakeholders, Establish a big data information security monitoring system and set up emergency plans, Ensure the normal development of big data technology and the level of information security.

References
[1] Haiyong Sun, Qing Li. Research on Big Data Information Security Risk Framework and Countermeasures [J]. Information and Computer (Theoretical edition), 2017(5):209-210.
[2] Xingang Zhang, Bo Yu, Baoping Wang. Typical risks and guarantee mechanisms of big data information security [J]. Innovation and Technology. 2016(10):75-77.
[3] Shuai Wang, Huamin Jin, Jun Shen. Research on Security Schemes and Countermeasures of Big Data Application [J]. Guangdong Communication Technology. 2017, 37(8):2-5.
[4] Yan Tian, Xingang Zhang, Gaohua Wang, et al. Information security risk analysis and countermeasures in the big data environment [J]. Innovation Science and Technology, 2017(6): 31-33.
[5] Jialu Hou, Yonggang Guo, Xiaofeng Hu. Analysis of Information Security Issues in the Big Data Era [J]. Curriculum Education Research: New Teacher Teaching. 2015(22).
[6] Mingyue Wang, Xing Zhang, Wanjie Li, Qingyun Zhang, Xiaohui. Li Overview of research on privacy protection technology for data release [J]. Small Microcomputer Systems, 2020, 41(12): 2657-2667.
[7] Sheng Ji, Yizheng Liu, Xiaoshu Liu. Escort Qingdao to build the "World Industrial Internet Capital" with "Data Security"[N]. Qingdao Daily, 2020-12-12(004).
[8] Xin He, Yunxia Gao. Research and Implementation of Sensitive Data Identification Method Based on Feedback in Big Data Environment [J]. Telecommunications Engineering Technology and Standardization, 2020, 33(12): 54-59.
[9] Qianchuan Wang, Qingyong Chen, Cheng Zhang, Yu Zhang. Research on the security protection of medical privacy data in 5G cloud-side collaboration scenarios[J].Telecom Engineering Technology and Standardization,2020,33(12):64-67.
[10] Yulong Yang. Big data cannot turn the public into "transparent people"[N]. Health News, 2020-12-10(002).
[11] Jiang Jie. Privacy risk and regulatory measures of big data rotation[J]. Information Science,2014(6): 18-23.
[12] Victor Meyer-Schoenberger, Kenneth Cookeer, Sheng Yangyan, Zhou Tao Translation. The era of big data-great changes in life, work and thinking [M]. Hangzhou: People of Zhejiang Publishing House, 2013.
[13] Ma Jiantang. Earnestly grasp the new opportunities and new changes in the era of big data [N]. Economic Day Newspaper, 2016-01-11 (14).
[14] Liu Dehuan, Li Xuelian. The risks and existing problems of big data[J]. Advertising Grand View: Li On the edition, 2013 (3): 67-73.