Challenges and Solutions of Information Security Issues in the Age of Big Data

YANG Mengke[1,2*], ZHOU Xiaoguang[1], ZENG Jianqiu[3], XU Jianjian[3]

[1]School of Automation, Beijing University of Posts and Telecommunications, Beijing100876, China
[2]School of Computer Science, Beijing University of Posts and Telecommunications, Beijing100876, China
[3]School of Economics & Management, Beijing University of Posts and Telecommunications, Beijing100876, China

Abstract: Big data has been taken as a Chinese national strategy in order to satisfy the developments of the social and economic requirements and the development of new information technology. The prosperity of big data brings not only convenience to people's daily life and more opportunities to enterprises, but more challenges with information security as well. This paper has a research on new types and features of information security issues in the age of big data, and puts forward the solutions for the above issues: build up the big data security management platform, set up the establishment of information security system and implement relevant laws and regulations.

Keywords: information security; big data; data privacy; information technology

I. INTRODCUTION

On September 5, 2015, the State Council of China issued guidance to boost the development of big data, officially taking big data as a Chinese national strategy. Big data is a broad term for data sets since it is so large and complex that traditional data and its processing applications cannot be compared. Generally speaking, big data refers to the information assets characterized by high volume, velocity and variety to require specific technology and analytic methods for its transformation into value[1]. As a revelatory exploration of the practical application of information technology, big data will have a dramatic impact on economy, science and society based on the policy that is firmly committed in China [2].

The rapid growth of big data not only brings convenience to people's daily life, but also great opportunities to enterprises. For example, under the help of the big data boom, Microsoft establishes its own intelligent data management system based on big data and produces a kind of data-driven software mainly to save energy and promote efficiency, which can save 40% energy for this application. It seems that big data is becoming the huge economic assets, and will bring new entrepreneurial opportunity, business model and even innovation thinking all over the world.

However, big data also brings challenges, especially for the information security due to its distinct characteristics (shown in Figure 1). First of all, big data may increase the risk of information leakage because of its high volume and velocity that Prism is a striking example which shows that one person or one set of computer can cause a serious consequence by big data analysis. Meanwhile the fast development of intelligent terminals is along with the growing risk of information leakage. This relates to the privacy, prediction of people's behaviors while using these terminals, sometimes it even threatens the safety of a country. In addition, with the application of social contact data is in openization and exposed to the hackers, this makes big data an easy target to attack since all these data is correlative to each other, if hackers make one of these correlative data as the carrier of virus which cannot be found in time, the damage will be immense. Furthermore, owing to the feature of variety for big data, not all of the data is structured data and the unstructured data either does not have a pre-defined data model or is not organized in a pre-defined manner, while traditional database and data processing cannot meet the demands of the storage of unstructured data which is typically text-heavy, but may contain data such as dates, numbers, and facts as well. And with the fast expansion of data size, various data will gather together, which makes the traditional storage and management measures invalid [3,4].

Owing to these information security issues, how to deal with these challenges becomes an important problem. Therefore, this paper focuses on the solutions to these issues in the age of big data.

This paper has a research on new types and features of information security issues in the age of big data, and puts forward the solutions for the issues.

II. Research Status

International research on information security starts from related technology almost 50 years ago and it mainly experiences three periods. The first period begins in 1970s and scholars pay attention to the security of computer operating system[5]. The second period is in 1980s. American scholars put forward the earliest architecture principle of computer security system, TCSEC [6]. The third period starts from 1990s. Based on the improvement of TCSEC, formal analysis method which regards security protocol as important contents for information security becomes popular. With the rapid development and spread of information and communication technology, foreign scholars pay more attention to the application of new techniques in the field of information security. For example, Jong Hyuk, et al defines the security risks of smart-phone and puts forward an enhanced smart-phone security model based on Information Security Management System (ISMS) [7].

Likewise, domestic scholars mainly focus on the related technology based on the developing trend of the industries relative information security. Among these researches, the first is cryptography. It is divided into two types which are cryptography classified on mathematics and non-mathematics based on the differences of technological base. Domestic scholars make a deeper research in public-key cryptography, authentication code and sequence cipher. While compared with foreign research, there is still great gap. For example, China hasn't established its own standard system up till now and doesn't have normative documents to restrain and promote its development. Owing to the importance of security management, some scholars did the research from the aspect of security policy and legislation. For example, QinHao puts forward that the safer way to solve the problems of information security is to establish and complete related laws [8].

Nowadays, since the development of big data with such a blistering speed brings new challenges for information security, both domestic and foreign scholars pay more attention to the study on security of big data. It has become a sociological problem when data about personal information is collected and mined by companies such as Facebook, Google, mo-

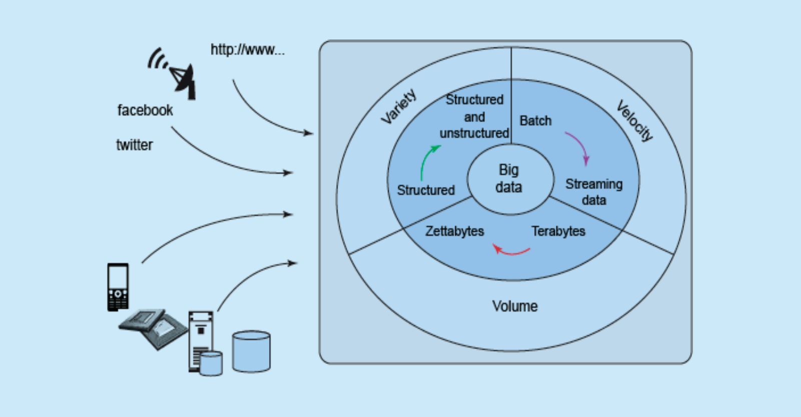

Fig.1 *Characteristics and challenges of big data*

bile phone companies, retail chains and even governments websites[9].And an encrypted search and cluster formation in big data was demonstrated in March 2014 at the American Society of Engineering Education.Gautam Siwach engaged at *Tackling the challenges of Big Data* by MIT Computer Science and Artificial Intelligence Laboratory and Dr. Amir Esmailpour at UNH Research Groupfocused on the security of big data and proposed an approach for identifying the encoding technique to advance towards an expedited search over encrypted text leading to the security enhancements for big data[10].Nevertheless, the research on information security facing big data has just begun in China that needs to be more thorough and specific implement. So the following is to study the current challenges of information security issues in the age of big data to figure out the solutions.

III. Current Challenges of Information Security in the Age of Big Data

Big data changes the nature of information security. The collection and storage of abundant or large data including IP address of customers, the budget of companies, and key information of governments result in the risk of information leakage, new irresistible targets for hackers, cyber thieves and terrorists to launch attack.

3.1 Big data increases the risk of information leakage

Data of cyber space covers vast range, such as sensors, social network and emails. The gathering of data inevitably increases the risk of information leakage. Big data provider huge information but the save of these gathering data which includes abundant records of government's information, business data and customers' information increases the risk of information leakage, and if these data is abused, it will threaten personal, firm and state safety. Meanwhile, there is no explicit limit of the ownership and the right to some sensitive data that is still the risk of information leakage. And this is why much analysis based on big data involving information leakage is really a current challenge of information security that threats for personal privacy and national safety in the age of big data [11].

3.1.1 Threats for personal privacy

The risk on information leakage will lead to the threat for personal privacy. On the one hand, the rapid development of information and technology brings convenience to people's daily life and provides more opportunities for enterprises while personal privacy such as the information of various behaviors is in leakage even every second. On the other hand, the universal application of new information technology increases the threats of the leakage of important personal information, such as the house address and phone number provided at the time of reception, password and information of credit card at the time of online shopping[12,13]. On March 22, 2014, WooYun Vulnerability Platform released the information that there are some bugs or loopholes in the payment system of Ctrip, which may cause the leakage of users' personal information including address name, ID number, types of credit card, CVV of cards. The leakage of these information will cause inconvenience to people's daily life and even cause property loss.

In the age of big data, the access permission of personal data becomes obscure. The leakage of privacy includes both personal information and predicting people's status and behavior.

3.1.2 Threats for national safety

The rapid development of information technology makes it easier to leak the information on the Internet, various intelligent terminals and portable storage devices, and the leakage might have a great influence on the safety for individuals, enterprises and the state. For example, China official media reports the details of the information leakage of DF-31 ICBM. It involves seven top-secret documents which are leaked to Taiwan. This issue influences greatly on the state safety and national defense construction.

3.2 Big data becomes the obvious target of cyber attack

In the cyber space, database integrated by big data is easier to become the target of hackers [14]. First of all, the huge amount of integrated data makes the hacker who successfully attacks the database obtains more data and decreases the cost of the attack. In addition, big data means more complicated and sensitive data, which is more attractive to hackers. Besides, the hacker can launch APT (Advanced Persistent Threats), while it is hard to be detected by the traditional protection strategy.

For example, on January 21st, 2014, a wide range of DNS in China broke down. According to the data delivered by some websites, there were 2/3 websites' DNS Server failing to work at the peak of this fault, which made thousands of Internet citizens fail to get on the Internet. This fault involved the tourist industry, aircraft industry, e-commerce and IT service etc. And all these websites showed "unable to establish the connections with your server". According to the data analysis by CNCERT, it is probably attacked by the hacker and that causes the failure of some websites.

3.3 Big data challenges existing save and security measures

Big data brings new security issues for save measures due to its variety. First of all, present data storage model only applies to the structured data, while most data is semi-structured or unstructured. This brings great challenges to traditional data storage manner since big data means to gather various and abundant data. For example, design data, customer information and operating data are always put together, and this might cause some troubles for the management of enterprises such as business security. Besides, for the mass data, regular security scanning measures need too much time to check the potential threats, and they cannot satisfy the demands that companies provide. What's more, the updating speed of security protection measures cannot catch up with the growth of mass or large data therefore, there must be some loopholes needing help in the protection of big data.

3.4 Big data is used as an attacking measure

Hackers use big data technology to launch an attack to companies when these companies use big data to obtain information for commercial value. Hackers try to get and base the information, such as social network, emails, microblog, e-commerce, phone number and address, to prepare for the attack and this can make the attack more accurate and result in big loss. In addition, there exist opportunities for hackers to attack based on big data. Hackers use big data to launch bonnet exploit, which may control millions of computers and launch attacks at the same time, and the traditional attack does not have this function or order of magnitude.

For example, in 2013, Spamhaus, an organization of anti-spam, suffered the most serious attack of DoS in the history of the Internet after it put Cyber bunker into blacklist of spam. In this attack, the aggressors adopted DNS reflect attack to magnify the attack traffic to 100 times easily under the help of abundant DNS servers. The attacker disguised the information as the message delivered by Spamhaus and distributed these messages to the servers, then these messages were magnified rapidly, and caused serious problems.

In addition, big data is used as the carrier of the virus. The hacker hides the attack like APT and this makes it difficult for the traditional protection measures to detect the attack. Traditional detection is real-time matching detection based on the features of detection, while APT is a process and it doesn't have obvious features that can be detected in real time. Meanwhile, the code of APT attack is hided in big data which makes it hard to be detected in detail. Moreover, it is very hard to focus on the value point for the security analysis device because of the low density value of big data, and this causes many troubles to the analysis of security service providers.

IV. Solutions to Protect Information Security in the Age of Big Data

For the development of networks convergence and Internet plus, social informatization has being permeated into every field and the information security issues are more prominent than ever before. Facing with the threats and challenges of information security in the age of big data, government and enterprises should do more and the solutions including establish big data security management platform, speed up the establishment of information security system and improve people's awareness in order to guarantee information security.

4.1 Establish big data security management platform

This paper divides big data security management platform into five layers: data storage layer, data processing layer, interface, data application layer and data management layer shown in Figure 2.

4.1.1 Data storage

Why data storage is an important layer is that the secure storage of big data uses virtualization to store mass data. And this involves data transmission, isolation and restoration. To deal with the secure storage of big data, data encryption is the first step [15]. In the design of big data security service, big data can be stored in any space of data set according to demands of data secure storage, and by SSL (Secure Sockets Layer), encryption, the knot of data set and application programs can protect the big data together. During the process of the transmission service of big data, the encryption provides effective protection for the upload and download of data stream, and uses privacy protection and outsources data calculation to shield cyber-attack as well. The second is to divide secret key and encrypted data, and apply encryption to divide data use and data storage, and to separate key from the data that needs to be protected while to definite the life-cycle of the secret key management of the emergence, storage, backups and restoration. The third is to use filter. The transmission of data will be stopped once the data leaves client's network. The fourth is data backup. Under the help of disaster tolerant system, centralized management of sensitive information and data, the data protection from end-to-end will be realized.

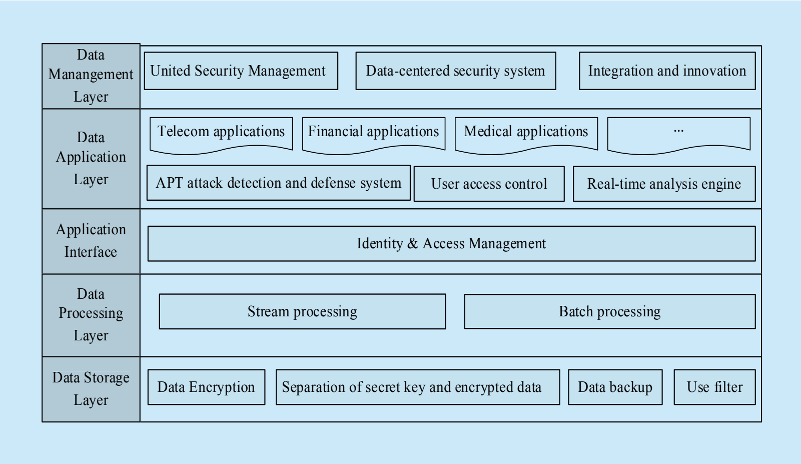

Fig.2 *Big data security management platform*

4.1.2 Data processing

Data processing is the core of big data technology, which has an impact on the information security directly. The attack like APT can be prevented by the effective data processing technology such as real-time stream processing. In general, the main processing mode of big data can be divided into stream processing and batch processing.

4.1.2.1 Stream processing

The basic concept of stream processing is that the value of data will decrease along with the flying of time being, therefore, it is a common subjective of all stream processing to analyze the newest data as soon as possible. It is mainly used in real time statistics and sensor network.

Stream processing regards the data as a stream. When new data comes, it will be analyzed right away and return the results needed. The basic mode of stream processing is shown in Figure 3[16].

4.1.2.2 Batch processing

MapReduce, presented by Google in 2004, is a classic batch processing. The whole process of MapReduce is as follows. First, MapReduce divides the original data into several sections, and then these sections are dealt with different Map task areas. Map task gets corresponding result and executes Map function that is user defined, and then the results will be recorded into local disk. After that, Reduce task will rank according to the Key value after it reads data from the disk. The same key value will be put together, and the user-defined Reduce function will deal with the sequenced result and output the final results, as is shown in Figure 4[17].

4.1.3 Interface of Big data

Big data needs to pay attention to interface and coordination of data diversity is an inevitable issue with the development of Internet applications. As an important link of data processing, it is necessary to unify the access interface. However, how to protect the security of the interface is to the security issue. To solve this problem, this paper gives the suggestions as follows.

IAM (Identity & Access Management) is a set of business process and management measures for providing efficient and secure IT resource access[18]. It provides unified authentication strategy and guarantees the correct security level of Internet and application program of local area network, and this can make sure that the application program of high security level can be protected by more advanced authentication method. In addition, IAM designs different access rights for every client. Users can visit the data with relevant permission. Meanwhile, it can change the permission level according to users' behavior in order to avoid consistent great loss once the authorized accounts are stolen.

Besides, the security of the interface needs the support of VPN encryption technology and background linkage of managers including remote lock, data wiping and automatic alarm.

4.1.4 Security of big data application

Big data has a wide range of applications, such as telecom, finance, health care, and the security of big data application is very important in protection.

With the fast development of the technology and tools of big data application, the strategy of big data application security should be considered from the following aspects. The first is to prevent APT attack aiming at big data application platform. APT attack detection and defense system should be designed to alarm the viruses under the help of big data processing technology. All the network access request can be stored in the form of big data, and then process behavior modeling, correlation analysis, and visualization of the enter-

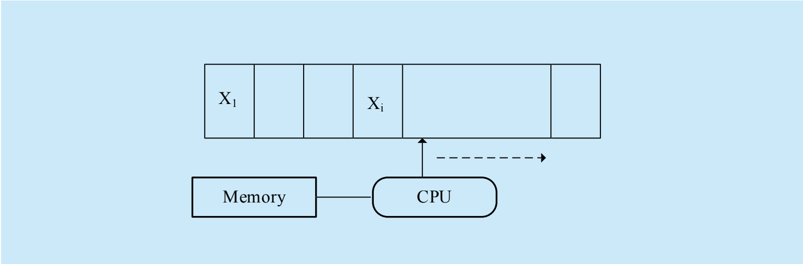

Fig.3 *Basic data stream model*

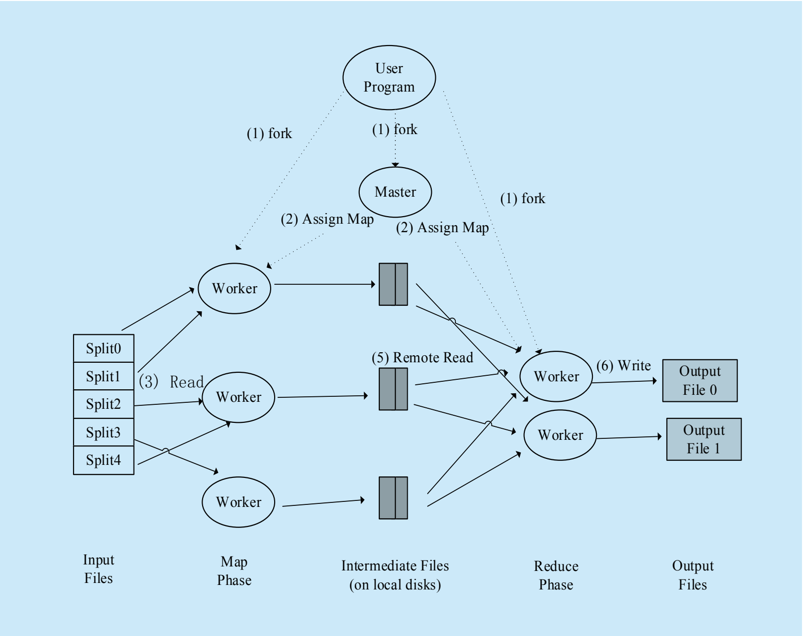

Fig.4 *Execution overview of MapReduce*

prise internal network access to automatically discover abnormal behavior of the network access request, trace and locate APT attack process. The second is user access control. The application of cross-platform transmission of big data has internal risk to some degree. Attribute-based encryption (ABE) which has emerged as a promising technique to ensure the end-to-end data security can help data owners to define access policy and encrypt the data, such that only users whose attributes satisfying these access policies can decrypt the data [19].In addition, the unified identity authentication based on SSO (Single Sign-On) will also be helpful for the big data application security. The third is real-time analysis engine. It includes cloud computing, machine learning, semantic analysis and statistics. The hacker attack, illegal operation, potential threats can be found and alerted at the first time under the help of data real-time analysis engine.

4.1.5 Big data management security

The security of big data not only depends on the advanced technology, but also requires management for the support as a solution.

4.1.5.1 United Security Management

The first is to establish a USM (United Security Management) system which is an active, visual system that provides integrated management for various security issues. It integrates the mainstream network security measures as a whole and all the issues are controlled by a management center. This will save the purchasing costs and maintenance costs. In addition, USM solves the problem that the Internet responses too slow to the new threats because of the differences of the security strategy and decreases the management tasks for the administrator. Furthermore, the report of query and analysis system of SAFEMAN collects all the secure report information of SPC database which is in the domain area. Then it will mine thesecure information of the network, and analyze various security threats in the forms of charts and figures according to the time. In this way, it makes the companies catch the whole security running state, and provides a solid foundation for the following security program as well.

4.1.5.2 Establishing a data-centered security system

The second is to establish a secure system which is data-centered. The big data based on cloud computing is stored in cloud share [20]. In order to make good use of big data, it is in need to establish a secure system which is isomerous data-centered, and guarantee the big data security based on this management system.

4.1.5.3 Integration and innovation

The third is integration and innovation. Big data is a new concept which is based on cloud computing. In the big data era, how to integrate the big data and cloud computing together and improve the scale, level and connotation of data traffic based on the smart pipe and aggregation platform is important for big data safety application.

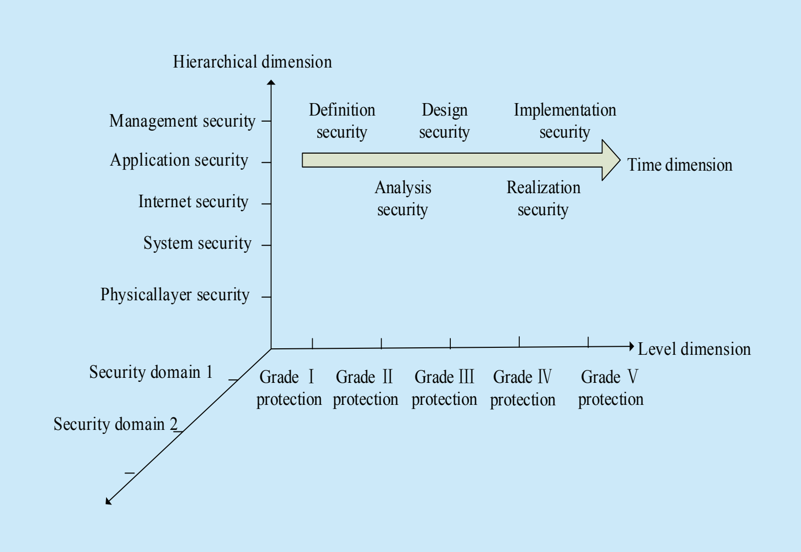

Fig.5 *Information security technology system*

4.2 Speed up the establishment of information security technology system

Different systems have different formations even for the same system, and this is why the information target which needs to be protected is different. Figure 5 is the information security technology system which shows that it needs to adopt protection measures from different security levels and establish scientific and reasonable information security technology system [21].

4.2.1 Layered protection

As is shown in Figure 4, the construction of information security system is formed through the expansion layers of computer hardware. The security of outer software system relies on the security of inner system. Any insecurity will influence the security of upper layer. If the ground layer is not secure, the subject will bypass the upper system and pass through the insecure ground layer to visit the objective information and this may form the bypassed information security threats which will result in the security of the whole system. For example, if the operating system doesn't have the security protection, since the data base has security protection, yet the system is still unsafe. Though the secure data base system can control the visit to the data, yet the data base system is established based on the operating system. Data base system puts these data on the hardware, while the operating system users can steer by the data base system, and visit the document that stores the data directly, and this may form the security bypass.

In addition, when these layered information security products form a system, it needs to pay attention to the dependence and complementary relationship. Security of lower layer products needs to support the security of upper layer products. The contradiction and incompatible phenomenon will not be happened.

4.2.2 Protection of different domains

Big data security has very close relationship with operation system and computer system for instance forms the distributed network system by the network. The protection target, strategy and technology of different domains are different; therefore, it is necessary to use different technology for different domains [22]. DNS can be divided into computing environment of local region, network perimeter, network transmission and network infrastructure, and illustrates how to use different technology in different secure regions to establish distributed information security system.

The computing environment of local region uses secure operating system, secure data base, intrusion detection and security authentication, network perimeter adopts firewall, physical isolation to prevent the attack outside. Network transmission uses security router and security protocol to guarantee the data security during the transmission. Security infrastructure like PKI/PMI provides secure service for the information system.

4.2.3 Hierarchical protection

The importance of the same information is different for different institutes; therefore, hierarchical protection is in need.

This concept came into being long time ago. According to TCSES, the computer system can be divided into 4 levels and 7 kinds. IOS divided information security assessment into 7 levels. The criterion, GB 17859-1999, classified by China divided computer information security system into 5 levels.

4.2.4 Timeshare protection

Information security of big data is a dynamic process. From the aspect of time dimension, the protection of information security can be divided into macroscopic protection and microcosmic protection.

Macroscopic protection means to enact laws, regulations and technology criterion of information security protection. Then the competent department authorizes related institute to assess the system according to the criterion. The third, the competent department and organization of information security protection supervise and check the operation of the system.

As for the microcosmic protection, information security is the security protection under the cognition to the threat, fragility of the system and management ability. And the ability of the protection technologies is limited and it is difficult to guarantee 100% safety. In addition, new attack technology and other security threats appear continuously. Based on this, in order to improve the ability of protection in the age of big data, it is possible to adopt dynamic information security protection and set up the information security model which includes the protection, detection and response based on time dimension. For instance, PDR (Protection, Detection, Response), the famous information security model, was first put forward by ISS company and then Chinese experts put forward WPPDRRC adding the warning and proactive function to guarantee the information security [23].

4.3 Implement relevant laws and regulations

Data privacy is a highly sensitive issue in the age of big data, and with the public becoming increasingly mindful of the risks of cybercrime and personal data breaches, the legislation of data protection becomes a task that brooks no delay. Therefore, firstly, it is a fundamental measure to implement relevant laws and regulations to strengthen the safety protection of the information networks and the key information system in order to ensure the safety of network data. Especially, the legislation of data resources rights should be put on the lawmaking agenda as soon as possible.

Secondly, it is essential to promote the legislation of online personal information protection, define the scope of the personal information collection and application, clear the rights, responsibilities and obligations of related subjects, and enhance the punishment of ill behavior such as invasion of privacy.

Last but not least, since people’s security awareness plays an important role in information security, personal information security awareness needs to be improved under the guidance [24]. So, to step up efforts in supervising administration and educate subscribers especially the adolescence, are practical measures to improve the information security awareness and regulate network behavior[25]. Only when information security awareness has been strengthened, can the improvement of information security be realized.

V. Conclusions

Big data is leading the information revolution with the development of information technology, and it has been taken as a national strategy in China. Yet the strategy may have problems that people still can’t enjoy the convenience from the benefits of big data if the security of information could not be guaranteed. Thus, information security is of great importance in the age of big data and the protection of the information security requires to set up the big data security management platform and system, implement relevant laws and regulations, and endeavors from Internet citizens of various smart terminals, and related legislature and network operators for the implement of information security in the age of big data.

Acknowledgements

This work has been partly supported by National Key Technology Support Program (No. 2013BAD17B06)and Major Program of National Social Science Fund(No.15ZDB154).

References

[1] DE MAURO ANDREA, GRECO MARCO, GRIMALDI MICHEL. What is big data? A consensual definition and a review of key research topics[C]. AIP Conference Proceedings.2015, 1644: 97–104.

[2] VIKTOR MAYER SCHONBERGER, KENNETH CUKIER.Big Data: A Revolution That Will Transform How We Live, Work and Think [M]. London: John Murray Publishers Ltd ,2013:10-18

[3] MARX, V. The Big Challenges of Big Data[J] .Nature,2013,498（7453）: 255-260 .

[4] WU Xindong, ZhuXingquan, Wu Gongqing, Ding Wei. Data Mining with Big Data[J]. IEEE Transactions on Knowledge and Data Engineering, 2014, 26(1): 97-107.

[5] ABBOTT R P, CHIN J S, DONNELLEY J E, et al. Security Analysis and Enhancements of Computer Operating Systems [J]. Security Analysis & Enhancements of Computer Operating Systems, 1976.

[6] STEVE LIPNER, The Birth and Death of the Orange Book[C] .IEEE Annals of the History of Computing.2015,2(37): 19-31

[7] JONG HYUK PARK, KI JUNG YI, YOUNG-SIK JEONG. An Enhanced Smart-phone Security Model Based on Information Security Manage-

ment System (ISMS) [J]. Electronic Commerce Research, 2014(14).
[8] QIN Hao. Research Status and Developing Trend of Information Security [J].Computer Knowledge and Technology. 2012, 8(31):56-58
[9] SMITH M, SZONGOTT C, HENNE B, ET AL. Big data privacy issues in public social media[C]. Digital Ecosystems Technologies (DEST),2012 6th IEEE International Conference onIEEE, 2012:1-6.
[10] SIWACH, GAUTAM, ESMAILPOUR, AMIR. Encrypted Search & Cluster Formation in Big Data[C]. ASEE 2014 Zone I Conference. University of Bridgeport, Bridgeport, Connecticut, USA,2014
[11] MACHANAVAJJHALA A., REITER J.P., Big Privacy: Protecting Confidentiality in Big Data[J]. ACM Crossroads, 2012,19(1):20-23
[12] THERESA PAYTON, THEODORE CLAYPOOLE .Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family [M]. Maryland:Rowman & Littlefield Publishers,2014
[13] MOHSEN ATTARAN ILIA VANLAAR, Privacy and Security on the Internet: how to secure your personal information and company data[J].Information Management & Computer Security, 1999(07): 241 -247
[14] GREGORY R. DODDRELL. Information Security and the Internet [J]. Internet Research, 1996(06): 5 - 9
[15] FENG Guodeng, Zhang Min et al. Big Data Security and Privacy Protection [J]. Chinese Journal of Computer. 2014, 37(1):27-31
[16] CHARDONNENS T, CUDRE-MAUROUX P, GRUND M, et al. Big data analytics on high Velocity streams: A case study[C]// Big Data, 2013 IEEE International Conference on. IEEE, 2013:784-787.
[17] DEAN J, GHEMAWAT S. MapReduce: Simplified Data Processing on Large Clusters.[J]. Communications of the ACM,2008,51(1) : 107 -1l3
[18] MARY MADDEN, SUSANNAH FOX, AARON SMITH, JESSICA VITAK. Digital Footprints: Online Identity Management and Search in the Age of Transparency[J]. Pew Research Center, 2007
[19] Yang K, Jia X, Ren K. Secure and Verifiable Policy Update Outsourcing for Big Data Access Control in the Cloud[J]. IEEE Transactions on Parallel & Distributed Systems, 2015,26(12):3461-3470
[20] ZHOU Ke, Wang Hua et al. Cloud Storage Technology and Applications [J]. National High Technology Research and Development Program of China, 2010(04).
[21] ROSSOUW VON SOLMS, Information Security Management: why information security is so important [J]. Information Management & Computer Security, 1998(06):174 – 177
[22] YU Zheng.Methodologies for Cross-Domain Data Fusion: An Overview[J]. IEEE transactions on big data, 2015,1(1):16-34
[23] ALCARAZ C, TURAN M S. PDR: A Prevention, Detection and Response Mechanism for Anomalies in Energy Control Systems [J].Critical Information Infrastructures Security, 2013:22-33.
[24] MARIANA GERBER ROSSOUW VON SOLMS PAUL OVERBEEK, Formalizing Information Security Requirements [J]. Information Management & Computer Security, 2001(09):32-37
[25] STEVE HAWKINS DAVID C. YEN DAVID C. CHOU. Awareness and Challenges of Internet Security [J]. Information Management & Computer Security, 2000(08):131 – 143

Biographies

YANG Mengke, is recently doing her post-doctoral research work at Beijing University of Posts and Telecommunications. She has received her PhD degree in management science and engineering from BUPT, and been involved in many scientific research including national key projects and enterprise consulting projects. Her major research interests include information technology management, e-commerce and logistics. *The corresponding author. Email:yangmengke@139.com.

ZHOU Xiaoguang, received master's degree in engineering from Tsinghua University, and PhD degree in Japan. He is now a professor at the School of Automation in Beijing University of Posts and Telecommunications. His major research interests include automatic logistics system, the technology and application of Internet of things.

ZENG Jianqiu, received PhD degree from University of Cambridge. He is now a professor at the School of Economics & Management in Beijing University of Posts and Telecommunications. He has been involved in the research of technical and economic management, competition ability and strategy for about 30 years, and published more than 10 books.

XU Jianjian, a postgraduate student at the School of Economics & Management in Beijing University of Posts and Telecommunications. His major research interests include information technology management, enterprise competitiveness and strategy.