Big Data Security and Privacy Protection

Dongpo Zhang

College of Computer and Information Engineering,

Zhengzhou University of Industrial Technology,

Zhengzhou Henan 451150, China

153396742@qq.com

Abstract.

In the era of big data, people's lifestyles, daily habits, and modes of thinking have undergone earth-shaking changes. Big data has become an important topic for research in industry and academia. But big data is a double-edged sword. It brings convenience to people and brings certain risks. In the process of data collection, storage, and use, it can easily lead to the leakage of personal information, and the fact that data is difficult to discern. How to ensure big data security and privacy protection has become one of the hot issues in the current stage of research. This article starts with big data, analyzes the security problems of big data, and proposes protection strategies for big data security and privacy.

Keywords: Big data; Security; Privacy

Introduction

In the era of big data, people are the beneficiaries of Internet technology. Data has great commercial value for Internet service providers, but the analysis and application of data will be more complex and difficult to manage, and personal privacy will be threatened. With the rapid development of the Internet, people leave a lot of data traces on the Internet every day. This gives criminals an opportunity to collect information on the Internet and then conduct illegal activities such as reselling, fraud, etc., not only for people. Life has brought troubles and brought economic losses, which has seriously affected social stability and harmony. In the era of big data, how

to deal with security and privacy issues in the context of big data is an urgent need for people to have a good solution.

Sources and Characteristics of Big Data

The origin of big data comes from the Internet. Researchers create diversified models based on the needs of the business, and then extract meaningful vectors based on the models to find ways to deal with people or things in different roles. This is the source and characteristics of big data. . According to the sources of big data, big data can be divided into three categories: First, all kinds of data that come from people, people in the process of using the Internet, including video, pictures, text, etc.; second, from the machine, each The data generated by various types of computers in the course of operations is in the form of multimedia, databases, GPS, smart homes, documents, etc. The third is from objects. The data collected during the operation of various types of digital devices, such as digital signals acquired by the camera.

Big Data Security Challenges

Privacy Risks. While people enjoy the convenience brought by big data, they also encounter a lot of inconveniences. If big data is not well protected for user data in the process of use, it will directly threaten the privacy of users and the security of data. According to different protection content, it can be divided into anonymous identifiers, anonymous protection and privacy protection. In the era of big data, people's data security problems are not only the traditional issues of personal privacy, but more based on the analysis and research of people's data, and the targeted prediction of people's state and behavior. For example, retailers can compare Parents are more aware of their children's spending habits, etc., and thus post relevant advertising information. Another example is the status

of content published by users on the Internet, and can analyze this person's political information, like the team, and spending habits. At present, many companies believe that after the information is processed anonymously, the identifiers will be hidden, and then the information will be released. However, the reality is that the protection of privacy cannot be effectively achieved only through anonymous protection. For example, a company may use some of its search history records in an anonymous manner within 3 months for use by people. Although the identification information contained therein has been carefully handled, the contents of many of the records contained therein can be accurately defined. Positioning. At present, China still lacks rules and regulations for user information management under the era of big data, and

it does not have a good supervision system. This, coupled with the lack of self-protection awareness among users, has caused many losses caused by information leakage.

Big Data Credibility Needs to be Confirmed.

It is generally believed that although data can explain some problems to a certain extent, the data itself is a fact, but the reality is that if the data can not be effectively screened, people will be deceived by data. One is that criminals can intentionally fabricate and forge data in big data. The basis of big data analysis is these data, and wrong data will inevitably lead to erroneous results. If the data use scenario is more specific, some people may make up the data to create data illusions that are beneficial to them, leading people to make wrong judgments. For example, some websites contain false comments, and users can easily buy these inferior goods and services after seeing these fake comments. Coupled with the current popularity of Internet technology, the impact of these false information is immeasurable, and the use of information security technology to screen these data is also very difficult. Second, big data may be distorted during the process of propagation. This is mainly due to the fact that information may gradually be distorted in the process of information dissemination. Therefore, ensuring the authenticity and reliability of data is extremely important.

Big Data Privacy Protection Technology is Lacking.

In the era of big data, information is disseminated at an extremely fast pace. At the same time as the transmission of information, due to the weak supervision of data information, lack of technical support, imperfect supervision system, and the vulnerability of information loss, the use of data information is not of high value and data is reduced. The value of itself will bring about many negative and negative effects on individuals, businesses and even the society, resulting in greater economic losses.

Threats to Data Security.

From the dawn of the era of big data, and the explosive growth of the Internet, this kind of network environment makes the security of mobile data of intelligent data terminals themselves more and more important. The current China has become the world's largest market for smart mobile terminals. These large numbers of mobile terminals not only occupy people's energy and time, but also store more personal data internally. At present, people have serious problems with the security of big data, and think that big data is not safe. Not just the trouble caused by big data. The security problems of personally-carried intelligent terminals are also very worrying. Therefore, the security of smart terminals has also become a serious problem for

users. Smart products are also evolving from current personal smart terminals to smart homes. The user's personal intelligent terminal can control the home terminal product later. Then, once the personal mobile terminal is controlled or lost, it will bring serious security problems to the user's smart home.

Big Data Security and Privacy Protection

Fully Supervise Data Information in Social Networks.
The online media that was created in the era of big data has become the most important channel for interpersonal communication. Strengthening supervision of data information is extremely important. First of all, it is necessary to strengthen the supervision and management of data and anonymously protect the network data for anonymous social media; secondly, to conduct supervision and management of social information so as to ensure that personal information security is not exploited by criminals and cause greater losses. Moreover, to increase users' awareness of safety precautions and minimize the filling of personal important information, self-prevention awareness and vigilance pitfalls are also needed.

Finally, the government should introduce better rules and regulations for the application of big data as soon as possible, and strengthen the legal aspects.

Improve the Privacy Protection Legal Mechanism.
With the development of society, people pay more and more attention to privacy, and China also pays more attention to the protection of individual privacy rights of citizens and puts forward many measures for the protection of information. In the "Criminal Law Amendment", the regulations for the protection of citizens' personal information are explicitly proposed, that is, no matter what the public officer knows about the citizen's information, he must not use any means to give information to others. If the citizen's information is leaked due to its own reasons, it needs to bear some legal responsibility. In our country's criminal law, not only regulations for protecting citizens' personal information have been proposed, but also penalties for obtaining information from others or leaking information from others have been added. However, at present, there is no law that specifically protects private information in our country's laws. Therefore, in order to better protect the security of big data, the government needs to establish a comprehensive privacy information protection law to protect citizens' personal information.

Establish a Privacy Protection Agency.

Most western countries have established special privacy protection agencies to protect citizens' privacy and information. By establishing a privacy protection agency, not only can people's online behavior be effectively monitored, but also the purpose of popularizing the law. Analysis of the current state of development in China, although the government has established functional departments for the protection of privacy issues, such as the Public Security Bureau, the Ministry of Industry and Information Technology, etc., but privacy protection is only one of these departments is not valued, and specialized privacy protection agencies have not been established. Therefore, it is necessary to establish a professional privacy protection agency for privacy affairs protection, so that it can fully play its role, protect the privacy of citizens, and effectively crack down on infringement of citizens' privacy and build a safe and harmonious life.

Improve People's Awareness and Quality of Data.

With the continuous advancement of the big data era, the number of data information has increased significantly. Citizens need to adapt to changes in the times and gradually increase their data literacy and data awareness. Data literacy is mainly aimed at scientific researchers and civil servants. It requires that when they are in contact with citizens' information, they can effectively manage citizens' information, and take the initiative to assume the responsibility of protecting citizens' privacy so that citizens' privacy can be effectively protected. The data awareness is mainly directed at the general public and requires citizens to realize the importance of big data. Do not arbitrarily publish information concerning their own privacy on the Internet, and do not casually publish other people's information so that they are not exploited by criminals. To the privacy of others, causing economic losses to others

Summary

The advent of the era of big data has not only provided important opportunities for social progress, but also brought a lot of information security threats to the society, making the protection of personal data privacy a concern. To realize the security and privacy protection of big data information, not only a large number of professional private information security technologies are needed, but also the awareness of privacy protection of citizens in our country needs to be strengthened so that privacy information security can be implemented.

References

[1] Fan Yan. Big Data Security and Privacy Protection [J]. Electronic Technology and Software Engineering, 2016(1): 227.

[2]Feng Dengguo, Zhang Min, Li Yu. Big Data Security and Privacy Protection[J]. Chinese Journal of Computers, 2014, 37(1): 246-258.

[3] Huo Honghua. Exploration of Security and Privacy Protection Technology in the Big Data
Era[J]. Cyber Security Technology and Applications, 2016,11(05):79-88.

[4] Luo Ying. Research on Big Data Security and Privacy Protection [J]. Information Communication, 2016(1):162-163.

[5]Wei Kaimin, Weng Jian, Ren Kui. A Survey of Big Data Security Protection Technology. Journal of Network and Information Security, 2016, 2(4).

[6] Peng L, Fang W. Heterogeneity of Inferring Reputation of Cooperative Behaviors for the
Prisoners' Dilemma Game [J]. Physica A: Statistical Mechanics and its
Applications, 2015, 433:
367–378.