Journal of Physics: Conference Series

PAPER • OPEN ACCESS

RETRACTED: Research on Network Information Security and Privacy Protection in the Age of Big Data

To cite this article: Zhang Gao 2019 *J. Phys.: Conf. Ser.* **1237** 022092

View the article online for updates and enhancements.

Retraction

Retraction: Research on Network Information Security and Privacy Protection in the Age of Big Data (*J. Phys.: Conf. Ser.* **1237** 022092)

Published 23 September 2022

This article has been retracted by IOP Publishing following an allegation that raises concerns this article may have been created, manipulated, and/or sold by a commercial entity. In addition, IOP Publishing has seen no evidence that reliable peer review was conducted on this article, despite the clear standards expected of and communicated to conference organisers.

The authors of the article have been given opportunity to present evidence that they were the original and genuine creators of the work, however at the time of publication of this notice, IOP Publishing has not received any response. IOP Publishing has analysed the article and agrees there are enough indicators to cause serious doubts over the legitimacy of the work and agree this article should be retracted. The authors are encouraged to contact IOP Publishing Limited if they have any comments on this retraction.

Retraction published: 23 September 2022

Research on Network Information Security and Privacy Protection in the Age of Big Data

Zhang Gao

SiChuan Aerospace Vocational College 610100

Abstract: The rapid development of big data has brought more problems in network information security and privacy protection. This paper will study the specific network information security and privacy protection technologies in this context. The first part of this paper firstly discusses the connotation and characteristics of big data, and then puts forward the information security and privacy protection problems in the era of big data. The last part deeply studies how to solve the solutions corresponding to these problems.

1. Introduction

With the continuous development of computer technology and network technology, the concept of big data is no longer unfamiliar to people, and with the sharp increase in the popularity of smart devices, the integration of big data technology and other industries has become inevitable. Big data itself has a variety of data types, high-speed data processing and other characteristics will be able to effectively promote the development of these industries [1], but at the same time, because the big data concept and related technologies are in a period of rapid development, such technologies Widespread application will inevitably lead to a large number of information security problems. At the same time, big data will collect and analyze various types of data generated by users during the use of the Internet. If there is no effective privacy protection, the user's personal information will be leaked. It is very likely that it will be leaked and it will have a serious impact on users. In order to enhance the positive impact that big data can bring to China's social development on the basis of the original, the impact of big data on network information security and privacy protection is minimized, and the network information security protection method corresponding to big data is carried out. Research is very necessary. This article will be discussed in detail in the following sections.

2. Connotation and Characteristics of Big Data

2.1 Connotation of Big Data

By definition, big data refers to large and complex data that can be processed with new processing models. The source of big data mainly includes the following aspects: ①People. That is, text, images, videos, and other information generated when people use the Internet. ②Things. That is, data collected from various types of devices. ③Computer. That is, the data generated during the operation of the computer [2]. In the practical application of big data, the focus is not only on the collection of large amounts of data, but also on the processing and application of large-scale data, which in turn makes the data more effective.

2.2 Characteristics of the Actual Application Process of Big Data and Related Technologies

①Large scale. As of 2015, big data contains information that can reach 8ZB.②Strong diversity. The difference in data sources, forms, etc. determines that big data itself has a very strong diversity. ③ High speed. Big data processing can obtain the target information from a large amount of information at a high speed, which is an inevitable requirement of the information age. ④High value. Through the rational application of a large amount of data, the data itself will have a very high rate of return, creating higher value on the basis of the original. ⑤In addition to the huge benefits, big data will also have a negative impact on user privacy protection, information security, etc. [3], which is the main content discussed in this article.

2.3 Major Development Goals of Big Data

In combination with the current application of big data in various fields, the main application and development goals of this technology mainly include the following points: ①To assist people to understand things more deeply and to predict the future development direction of these things. And make decisions.②Better provide personalized service to users to meet the individual needs of users. ③Use big data to filter errors or false information to filter the information. Figure 1 shows the main application areas of big data at this stage.

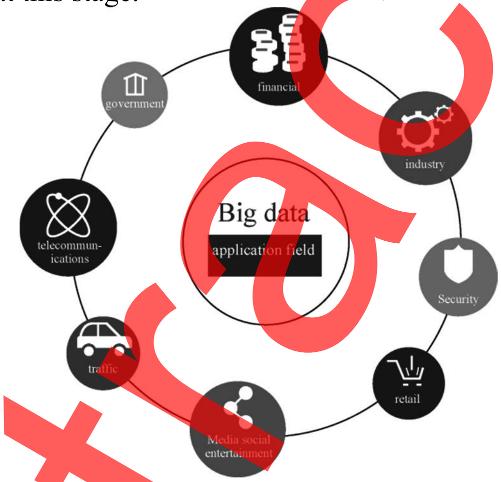

Figure 1 Big data main application areas

3. Major Network Information Security and Privacy Protection Issues in The Era of Big Data

3.1 User Privacy is Very Likely to be Leaked

With the help of big data, users' interests and preferences will be effectively speculated, and this feature has also been widely applied to various mobile APPs, so to more accurately recommend products or services to users. But without the management and control of this process, some enterprises are likely to use the collected data to predict user behavior or locate the user's location without the user's permission, which leads to serious violation of user privacy. For this point, the industry does not currently have a sound regulatory system for the rational application of big data. Privacy protection technology cannot meet the needs of users, which leads to a large number of privacy leaks, which seriously affects the development of users' normal production activities.

3.2 The Credibility of Big Data Still Needs Further Consideration

In the era of big data, information flooding is also one of the issues that need attention. Although the existing technology can effectively collect data from a large number of different types and sources, most of the data is authentic and reliable. Organizations do not conduct research in the actual application process, and if users use big data to make decisions, they are likely to cause serious losses or confusion to themselves. For this point, in order to ensure the effective application and continuous development of big data, it is very necessary to construct a special data authenticity inspection method.

3.3 The Database Lacks a Corresponding Regulatory Mechanism

During the registration process, users are often asked to fill in a large amount of personal information, and how this information will be used or where it will flow, most users are not able to know through effective means. Similarly, for enterprises or organizations that collect such information, due to insufficient attention to information security and privacy protection, most of these enterprises have problems such as inadequate management and supervision mechanisms and lack of corresponding privacy protection technologies. In the background, once attacked, there will be a large number of user privacy information leakage problems, causing serious impact.

4. The Main Technology to Improve The Security of Big Data Network Information

4.1 Anonymous Information

By definition, anonymous information mainly refers to personal information such as name, home address, telephone number, etc., and then this part of the data is stored as shared content. The provision of real-time traffic monitoring service is based on this type of information[4]. Although anonymous information technology can protect user privacy to a certain extent, as long as enough data is collected, user information will inevitably be identified. The existing research data shows that only 11 data can be extracted from the mobile phone network to identify the user's personal identity, while the fingerprint needs at least 12 reference points to identify. At the same time, only the time and place of the four credit card transactions are required to identify the true identity of the credit card holder through the information element. Combining these contents, it is not difficult to find that as long as the richness of data is continuously increased, the user's private information still has the possibility of being leaked. Therefore, relevant research units have conducted further research on technologies such as OpenPDS and SafeAnswers based on anonymous information technology, in order to protect metadata privacy.

4.2 Anonymous Protection Technology

Anonymous protection technology is mainly used in social networks. Compared with traditional social platforms, in recent years, anonymous social platforms such as Whisper and Secret have quickly attracted a large number of users, and Snapchat has also obtained the function of burning after reading. Combined with the above-mentioned types of mobile phone applications, the existing anonymous protection technologies are mainly divided into two types: user identity anonymity and anonymous user attributes. However, in the actual application process of this technology, an attacker can still speculate through other data associated with it. For anonymous users and anonymous information, relevant research units should further study ways to resist such speculative data attacks in order to ensure the effectiveness of anonymous protection technology applications.

4.3 Digital Watermarking Technology

Digital watermarking technology is essentially an encryption technology that enhances the security of information transmission by embedding certain identification information into the information. The application of this technology can effectively improve the security of network information, but it also leads to problems such as information redundancy and accuracy errors.

4.4 Role Access Control

Role access control mainly refers to the establishment of roles for users, and then associates roles with specific permission sets to complete user authorization, rights management, and so on. Early role access control rights management mainly adopted the "top-down" mode. Although this mode can effectively deal with the division of roles of corporate positions, when the amount of data increases and the complexity increases, the application of this technology will require a large amount of Manpower to complete the role division of work, but led to reduced efficiency and increased likelihood of problems. In response to such a situation, the "bottom-up" model can effectively solve such problems, namely role mining. In the context of big data, role mining technology will automatically generate roles based on user access records and other information, thereby providing personalized services for a large number of users, while estimating the security risks caused by users' deviation from daily behavior [5] Finally, the use of this technology to ensure the security of network information and user privacy.

Combined with the status quo, the application of this technology is mainly for the processing of data sets on a closed basis, and it is still unable to effectively analyze the dynamically changing data. In combination with the future development of big data, the relevant research units will take the processing of dynamic change data as the main research direction.

4.5 Risk Access Control Technology

This technology is mainly for all types of enterprises. If the information security cannot be effectively guaranteed during the operation of the enterprise, the economic benefits of the enterprise will inevitably be seriously affected. In the era of big data, enterprises must be able to do a good job in collecting, storing and managing big data. Risk access control technology is the main tool to assist enterprises to actively discover potential threats. Take the security tools introduced by IBM's Big Data Security Intelligence as an example. This tool can detect the internal or external sources of specific security risks, and on this basis, assist enterprises to make decisions. Through the detection of incoming mail content and data, this type of tool will be able to effectively analyze the employee's work status and their own emotions, in order to prevent internal employees from leaking business secrets.

4.6 Information Traceability Technology

As the name suggests, information traceability technology mainly refers to the trace of the source of information, and then combined with this content to determine the authenticity of the information. With the support of this technology, the credibility of big data will be effectively improved. Combined with the status quo, the information traceability technology is mainly accomplished by means of multi-bit mark method. Through the data calculation method and the data source record, the authenticity of the data can be effectively judged. For the development of big data, data traceability technology has played an important role in cloud storage scenarios, file traceability and recovery. In the follow-up research process, relevant researchers should use this technology with big data. Further emphasis is placed on ensuring that this technology works as expected.

4.7 Other Technologies

Other technologies here mainly refer to the introduction of policies and the establishment of specific control institutions. In combination with the above, in order to improve the security of network information and user privacy in the era of big data, relevant government departments must introduce specific control measures or build special control mechanisms in line with the characteristics of big data, so as to avoid the constant increase of big data in the market. This article focuses on the following two points:

①Build a special privacy protection agency. With the wider application of big data, some developed countries have established special network privacy protection institutions. For the construction of existing privacy protection institutions in China, these organizations have been unable to meet the protection of personal privacy in the era of big data. demand. In order to improve against such conditions, the privacy protection organization in the context of the era of big data should be able to meet the following requirements: First, this organization should have certain law enforcement functions, illegal access to data or abuse in the application of big data. Strict management and control of user privacy information, etc., to ensure that big data can better play its role under the constraints of specific laws and regulations. Secondly, this institution should assume the responsibility of publicizing and educating and popularizing legal knowledge, ensuring that more enterprises or organizations can realize the importance of protecting network information security, attach importance to the protection of network security risks, and fundamentally avoid the leak of user privacy information.

②Auxiliary enterprises improve the rationality of data utilization. The rational application of big data can create more benefits for enterprises. In the process of controlling this process, relevant management units should avoid forcibly prohibiting enterprises or related organizations from using user privacy data, but should be based on the original basis. These companies or organizations are properly guided to ensure the rationality of big data applications. In addition, the government should be able to establish special laws and regulations for the use of big data, stipulate the scope of use of big data, and classify the security privacy level for different information to ensure that enterprises can protect the information safety while applying user privacy information. Under such a control mode, big data will be able to play its role better, and network information security and user privacy will be better protected.

5. Conclusion

In summary, based on the simple discussion of the main network information security and user privacy protection issues in the era of big data, this paper mainly applies the process of big data through anonymous information, role access control technology and risk access control technology. The method of protecting user privacy and security has been studied in depth. In the process of subsequent development, in order to ensure that big data can better play its role, relevant research units must be able to attach importance to network information security issues in the context of big data, and government departments should assist in the construction of specific laws and regulations. Individual enterprises or organizations can use big data to work reasonably, and fundamentally avoid user privacy violations.

References:

[1] Gao Yu, Li Li. New Features and Requirements of Information Security in the Age of Big Data [J]. Electronic Technology and Software Engineering, 2018 (24).

[2] Zhang Jian, Yang Jian. Computer network information security and protection in the era of big data [J]. Electronic Technology and Software Engineering, 2018 (24).

[3] Zhang Gang. Computer Network Information Security and Its Protection Countermeasures [J]. Electronic Technology and Software Engineering, 2018 (24).

[4] Li Xiaoxia. Computer Information Security Precautions Based on Big Data Era[J]. Electronic Technology and Software Engineering, 2018(24).

[5] Liang Zhiwen. Construction of Computer Information Security Processing System in Cloud Computing Mode[J]. Electronic Technology and Software Engineering, 2018(24).