

## Privacy Protection Method in the Era of Cloud Computing and Big Data

Ying Liu

*College Mobile Telecommunications, Chongqing University of Posts and Telecom, Chongqing, Sichuan, China*

**ABSTRACT:** Cloud Computing has become the academic and industrial hotspot in China in recent years. Cloud Computing can help business clients manage finance more conveniently and efficiently. It can also reduce the protection of privacy. In addition, its inherent deficiencies also hinder its application in the privacy protection such as safety, different criteria, etc. This paper analyzes the application of cloud computing and big data in privacy protection and the existing problems, and therefore puts forward ways to promote the privacy protection in the era of cloud computing and big data.

**Keywords:** privacy protection; cloud computing; big data

### 1 INTRODUCTION

With the era advent of cloud computing and big data, the Internet will always release massive amounts of data. A large number of economic and political interests are hidden behind the large amounts of data, particularly through data integration, analysis and mining, the power of data integration and control they exhibit has been far more than ever before. Big Data is like a double-edged sword, which makes the community has benefited from the use of big data, but privacy is also easy to be invaded.

At present, various countries have begun to pay attention to the protection of personal privacy. This suggests that accompany technological innovation generated cloud computing and big data era also spawned social sectors Privacy strong demand, which also constitutes an integral part of social progress. Cloud Computing has appeared as a new IT concept in the last few years.

At the end of 2007, IBM announced its plan for Cloud Computing. And on June 9 of 2011, during "2011 Cloud Computing Industry Development Summit Forum and Establishment Congress of Cloud Computing Professional Committee in China", Professional Committee of Cloud Computing of Computer Industry Association was formally established. As a result, an increasing number of enterprises have engaged in the development and application of Cloud Computing Industry. After AIS, the Cloud Computing Company will become the development trend in the next generation of enterprise accounting information, and it may help promote the enterprise accounting information construction to apply Cloud Computing. Cloud Computing is the fundamental change happening in the field of Information Technology. It is a representation of a movement towards the intensive and large scale specialization. On the other hand, it brings about not only convenience and efficiency problems, but also great challenges in the field of data security

and privacy protection.

As of June 2014, Chinese Internet users have reached 632 million, of which there are 527 million mobile phone users. According to statistics, over the past year, Chinese user's loss was nearly 150 billion yuan in the Internet, including attacks on the site, loss of privacy, false information and so on. 360 Center for Internet Security published that, daily average number of intercept Trojans is close to 1 million, more than 12 million blocking phishing attacks happen, and the number of false securities reaches 3,000,000, lottery fraud 4 million, fake website 5 million.

### 2 PRIVACY VIOLATIONS PERFORMANCE

First, privacy violations may be caused in the stored process of the data. Cloud service users can not know the exact location of data stored, and users of its personal data collection, storage, use and sharing cannot be effectively controlled. This may be due to different national laws and legal conflicts may also have data pooling and data loss.

Second, violations of privacy can be caused in the process of data transmission. Data transmission will be more open and pluralistic under the condition of cloud computing, and traditional methods of physically isolated area cannot effectively guarantee the safety of long-distance transmission, and electromagnetic leakage and eavesdropping will become more prominent security threats.

Third, privacy violations can be caused in the process of data processing. Cloud service providers may deploy a large number of virtual technologies, failure vulnerability and encryption infrastructure may generate new security risks. Large-scale data processing needs complete access control and identity management, in order to prevent unauthorized access to data, but the cloud service model dynamic sharing of resources will increase the difficulty of this management,

account hijacking, assault, identity camouflage, certification failure, the key lost so that it may threaten the security of user data.

Fourth, privacy violations can be caused in the process of data destruction. Simply deleting operation cannot complete destruction of data, because cloud service providers may back up the data, which similarly may not lead to complete destruction, and in order to meet the requirements of assist law enforce-

ment, national laws would normally require the service provider's data retention period and mandatory service that providers provide plaintext data available, but in practice, they are rarely restrained by collected limitation principle, conflict of public power and privacy risks need to be considered when the user select a point cloud services. Thus, in the era of big data and cloud computing, we should strengthen the protection of personal privacy.

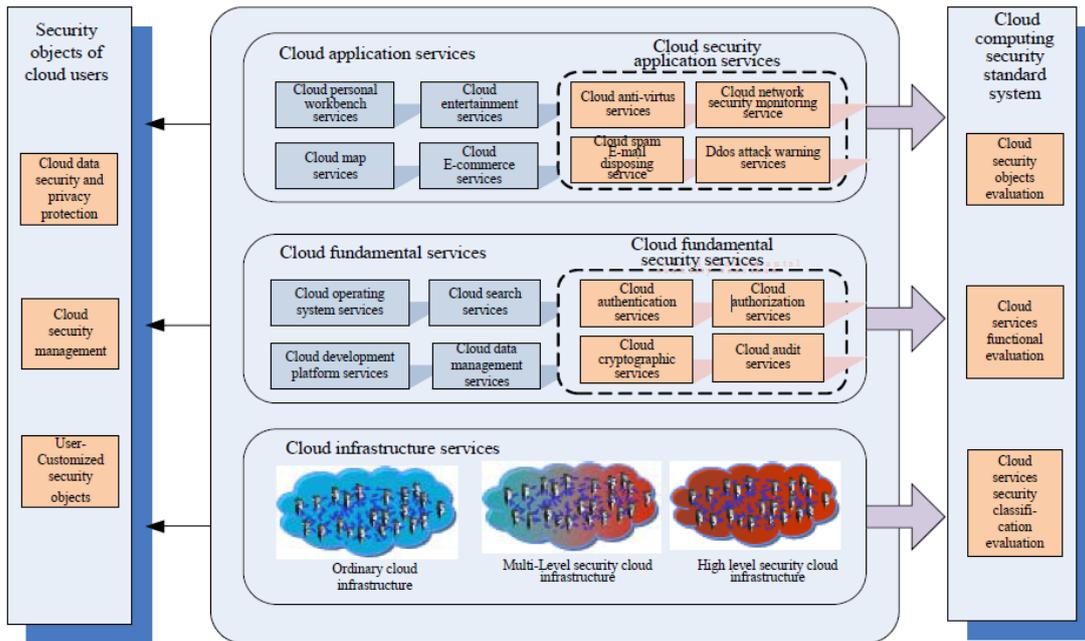


Figure 1. Cloud computing security framework

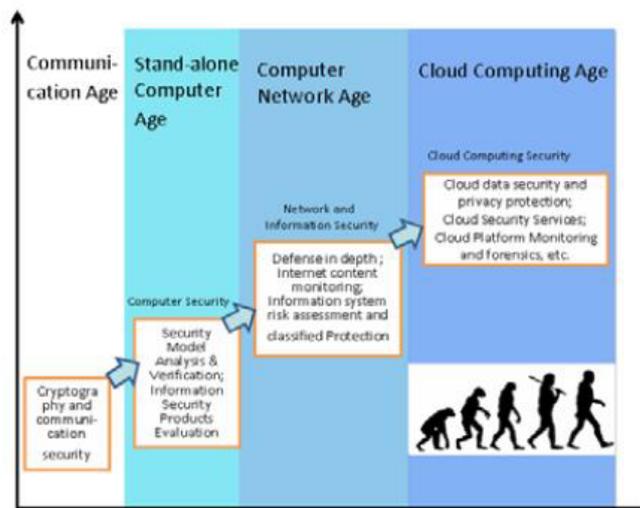


Figure 2. Evolution of information security technology

Before we propose the privacy protection methods, the cloud computing security framework can be seen in Figure 1. The cloud computing security mainly includes the following aspects: cloud application services, cloud security application services, cloud fundamental services, cloud fundamental security service and cloud infrastructure services. When we propose the suggestions of protecting our privacy, the above aspects should be taken into account seriously. In addition, we can see the evolution of information security technology in Figure 2. It can be seen that the cloud computing and big data security is of most significance in this era. So it is necessary to protect our privacy nowadays.

### 3 METHODS TO STRENGTHEN PRIVACY PROTECTION

First, the protection of personal information should be included in the scope of a national strategy to protect and plan resources. Privacy has formed the basis of modern business services operation and management of the network society in the cloud computing and big data era. For any country, their personal information is a strategic resource for development. At present in our country, from the network of systems, equipment, hardware to the operating system, application software, intelligent terminals and even chips and other core technology, they are still in a huge security risk, which is not only a threat to national security, but also have a serious threat to privacy for nearly half national number of citizens, which need to establish a personal information protection strategy and planning from the national level.

The second is to accelerate the legislation improvement of personal privacy protection. In the big data era, cloud computing technology is far less in terms of protection of personal privacy, we must establish laws and basic rules of personal privacy, and the lack of legislation in this regard is a serious problem that we currently have. It is necessary to actively promote privacy-related laws and regulations, legislation, to increase privacy acts against the crackdown.

The third is to strengthen the administrative supervision of personal privacy, and establish evaluation mechanisms of personal privacy protection and promote privacy and security of cloud service offerings relevant to national standards. In a network information environment, personal information and privacy has the property attribute, and for-profit companies may be stored in a cloud of privacy and other information for commercial use, resulting in leakage of user privacy and infringement. Therefore, it is very necessary to establish an effective government regulation. On the other hand, the state should actively promote the product in big data cloud service privacy and personal information security standards.

The fourth is to strengthen the technical protection of personal privacy. Technology is an important

complement to legal measures. The State and the community should actively encourage privacy technology development and innovation, from the technical level to protect privacy. In a variety of protected mode, PET are mature individual skills which is widely used at all levels, not only the protection of personal data, to prevent personal data from being unnecessarily treated, and let the user know where their data is stored, and how they are handled.

The fifth is to strengthen self-discipline and supervision. The relevant departments should actively promote cloud computing industry in the area of user privacy protection industry self-regulation, and to develop appropriate industry standards or conventions, to encourage and guide enterprises to participate in third-party industry organizations, and to provide policy and funding for the development of third-party organizations and other aspects of the industry.

In the era of big data, there are three principles in privacy protection. First, although the information is stored on a different server, you feel the ownership of these data belongs to whether these companies or the user. In the view of some researchers, these data should be the user's assets, which must be clear, just as property ownership. The future will have ownership of data privacy. Second, by use of Internet technology to provide users with all the information services, we need to collect user data secure storage and transmission, which is the responsibility and obligation of the enterprise. Third, if you want to use the user's information, be sure to let users have the right to know and the right to choose the so-called equal exchange, and authorize the use of disclosure of user data or profit, only to be regarded as immoral, but also illegal.

Cloud computing and big data also affects China's safety to some extent. According to reference [10], our satellite technology is private to protect our country. Once it is out, our national security will suffer great loss. Therefore, both our privacy protection and country's protection, we should take them into consideration.

The arrival of the era of big data and cloud computing makes the whole society be increasingly becoming a whole. In this system, privacy protection has become an important foundation for the construction of social credit system. We encourage innovation and progress, and simultaneously we must clearly see that both the United States and any other countries are selective disclosure and purposeful for the use of cloud computing and big data, not unprincipled to open, which is not only subject to laws and regulations limitations, but also with a country's overall development plan and global strategies which are closely related. Our efforts in the protection of personal privacy does not only protect against every member of society, but also for national security and long-term sustainable and healthy development of social protection.

## 4 CONCLUSION

With the era advent of cloud computing and big data, the Internet will always release massive amounts of data. Cloud computing and big data is emerging industry currently developing very rapidly, and has broad prospects for development, but simultaneously, security technology challenges they face are unprecedented. In this paper, the application of cloud computing and big data in privacy protection and the existing problems are analyzed, and some proposals are suggested to promote the privacy protection in the era of cloud computing and big data. The research of engineering protection in the era of cloud computing and big data is under way.

## REFERENCES

- [1] Liu C, et al. 2014. Robust  $H_\infty$  Control for satellite attitude control system with uncertainties and additive perturbation. *International Journal of Science*, 1(2): 1-9.
- [2] Distributed Management Task Force (DMTF) (in Chinese). <http://www.dmtf.org/home>
- [3] Cloud Security Alliance (in Chinese). <http://www.cloudsecurityalliance.org>
- [4] How to protect personal privacy in the big data era. [http://zqb.cyol.com/html/2014-09/25/nw.D110000zgqnb\\_20140925\\_3-02.htm](http://zqb.cyol.com/html/2014-09/25/nw.D110000zgqnb_20140925_3-02.htm)
- [5] Chang Y.C. & Mitzenmacher M. 2005. Privacy preserving keyword searches on remote encrypted data. In: Ioannidis J, Keromytis AD, Yung M, eds. *LNCS 3531*. New York: Springer-Verlag, pp: 442-455.
- [6] Liu C, Wang F. & Shi K, et al. 2014. Simulations for orbital maintenance of low-angle satellite based on STK. *Energy Education Science and Technology Part A: Energy Science and Research*, 32(6): 6307-6316.
- [7] Malek B. & Miri A.2009. Combining attribute-based and access systems. In: Muzio JC, Brent RP, eds. Proc. IEEE CSE 2009, 12th IEEE Int'l Conf. on Computational Science and Engineering. *IEEE Computer Society*. pp: 305-312.
- [8] Organization for the Advancement of Structured Information Standards (OASIS) (in Chinese). <http://www.oasis-open.org/>
- [9] Di Pietro R, Mancini LV. & Ateniese G. 2008. Scalable and efficient provable data possession. In: Levi A, ed. Proc. of the 4th Int'l Conf. on Security and Privacy in Communication Networks. Turkey: ACM DL. <http://eprint.iacr.org/2008/114.pdf>
- [10] Liu C. & Wang F. 2014. In-orbit estimation of inertia parameters of target satellite after capturing the tracking satellite.//*Intelligent Control and Automation (WCICA)*, 2014 11th World Congress on. IEEE, 3940-3945.
- [11] Zhou M, Zhang R. & Xie W, et al. 2010. Security and privacy in cloud computing: A survey[C]//*Semantics Knowledge and Grid (SKG)*, 2010 Sixth International Conference on. IEEE, 105-112.
- [12] Sabahi F.2011. Cloud computing security threats and responses[C]. // *Communication Software and Networks (ICCSN)*, 2011 IEEE 3rd International Conference on. IEEE: 245 - 249.
- [13] Liu C, Wang F. & Zhang Z.2014. Mixed  $H_2/H_\infty$  control for a satellite based on LMI[C]. // *Mechatronics and Control (ICMC)*, 2014 IEEE International Conference on. IEEE, 2114-2118.
- [14] Pearson S. Privacy, security and trust in cloud computing.//*Privacy and Security for Cloud Computing*. Springer London, 2013: 3-42.
- [15] Sweeney L. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 2002, 10(05): 557-570.
- [16] Tene O. & Polonetsky J. 2012. Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop.* 11.
- [17] Shi K. & Liu C, et al. 2015. Mixed  $H_2/H_\infty$  Approach of Full Order State Observer Design for Satellite Attitude Control System[C]//*Control and Decision Conference (2015 CCDC)*, The 27th Chinese. IEEE.
- [18] Kumar K V, Reddy D N C S. & Reddy B S.2015. Preserving Data Privacy, Security Models and Cryptographic Algorithms in Cloud Computing. *International Journal of Computer Engineering and Applications*, 7(1).