The legal fog around cloud computing agreements

Somayeh Sobati moghadam

Hakim Sabzevari University

Electrical and computer engineering faculty, Hakim Sabzevari University,

Sabzevar, Khorasane Razavi, Iran.

Sobati58@yahoo.com

Tel: 00985714003533

Abstract: *Cloud computing is a revolution in IT industry that attract many users to move their resources into a dedicated data centers with the accessibility via the internet. Cloud computing offers customers a large number of benefits that appeals the business or personal to switching on cloud. Choosing a suitable platform with a proper provider is a hard task because the customer don't have access to data center, thus there are the risk of data loss. Existing lows and rules have not always been able to go along with cloud developments. When a customer decided to have a contract with a cloud provider, the contractual argumentation about security is considerably high. Cloud agreements could appear in a vast variety of forms, however, there are a large number of juridical issues that should be considered by cloud customers. This article introduce the legalistic and contractual strategies to decrease the risks of outsourcing data.*

Keywords: Cloud computing, legal issue, privacy, security.

1. Introduction

Cloud computing offers a platform to address dynamically all rang of needs. It is able to provide a wide range of services for any kind of users and customers. It could be considered as a forward revolution in IT industry that is still immature. Due to its rapid growth, the legal and policy issues are not being widely discussed or addressed. As it is used in commercial and business purposes, it will be necessary to carefully consider the legal and contractual issues to avoid any detriment and damage for customers. Because of vast geographical locations of cloud data centers it could be accessible by anyone, anywhere which could cause the security problems. Cloud computing is a new common point in information technology and information legal. The existence legislation do not cover this new technology policy issues. Cloud computing does not a security offensive, but outsourcing data and move it outside of direct control could causes some security problem. In cloud computing the legal aspect is an important challenge for customers. Especially for the customers with sensitive data, the legal issues are more important thus it should be carefully addressed. In some countries there are a legislation to define the legal requirement in cloud framework. They worked according to data, specialization and geographical area. Their frameworks cover all sort of technology so their mandate will be covering cloud as well. Because of the nature of cloud the data are in danger in data center of cloud providers especially when the data are stored in the other countries that the customer is unaware of it. The customer transfer the burden of data management and protection to the cloud provider. The provider should assure the customer about data confidentially by applying the high and reasonable level of security. The essence of cloud computing make this more difficult and complicated because the provider is in association with the other supply chain. The customer don’t face with all the events, and it’s the final services which are important, but in the case of losing data the customer is the victim. In the case of disasters or threats which go along with data larceny, loss or deletion there is no guarantee to protect data. There is no anticipation in the continuum providers thus it’s just the customer that will suffer. The other problem is the different and uncertain geographical location of data centers. The customer‘s data would be located in different places in other countries with multiple litigation (Mangot, 2009). Different geographical places for storing data could cause the privacy threats. Also there are a similar trend in cloud legal, there are still much blind spot in cloud legal terms. In some countries like EU there are several limitation in data processing. The sensitive data like health or financial data need the owner permission to process on it. In this cases the data cannot be used in business (Mell and Grance, 2009). The EU countries don’t accept to store the data in the countries which are weak in security and don’t respect the privacy rights (Miras, 2002). They provided the essential to establish the security in other geographical location (Menascé, 2009). But without an international agreement it is impossible to impose the global rights within the cloud. The cloud providers use the customer‘s data for business purposes, the legal boundaries is indispensable. Thus without enforcing in cloud legal it is necessary that customer forecasts the probable threats and risks. Thus such problem should be addressed by provider and should be considered in contract. In this paper some of this problem that threats the security is introduced and the solution is proposed too. Customers are also strongly advised to consider the proposed solutions to achieve an acceptable level of security and Privacy .The customer could have different level of control of its data depends on cloud services. It’s vital to be aware of data security and privacy commitments especially in the case of sensitive data. If the suitable level of security has not been provided, it could be risky to transfer the sensitive data in cloud. The security measures should be considered in the contract to assure that there is no leakage in customer’s data. In the case of high sensitive data the access to data should be restricted to ensure that the provider’s persons don’t allow to act on data.

Additionally the customer should be ensure that the provider don't use its data for business purposes, it must be impermissible in the contract. The customer would be ensure that the provider is bounded to meet the security requirement.

2. Cloud computing (what is it?)

There are not a precise definition of cloud computing, everyone is thinking about it from its usage and perspective, but it means remote computing through the internet with accessibility to software which should be paid. Cloud computing is a migration from a traditional computing system with user's hardware and software resources to a new platform which use the other rental resources (Thompson, 2008). Cloud computing brings the fundamental change in computer world. It is considered as a revolution in the store way, software and tool development. Cloud computing brings a lot of advantages that has attracted many business.The main strength of cloud computing is costs benefits. Cloud can reduce the capital and operating cost because the resources are only paid for when used. Without cloud the customers have to buy enough hardware to meets their needs but with cloud they pay just for the services which used and it would be really economical. The large data centers has been built to handle the customer's needs. There are a great numbers of data centers with all equipment necessary for storing, cooling networking, etc. Through could the customer no longer have to be engaged in infrastructural details such as providing, configuring, managing which allows them to concentrate on main business trends? To serve a large number of user, the resources in cloud are pooled. The multi-tenancy feature of cloud allows to allocate the resources dynamically. The customer don't know about the exact location of data. On-demand service is another trait of cloud which allow customer to perform the tasks when they needed without any interaction with provider. Some customers are caution about security and privacy of cloud. Cloud computing could be used in two most general way. In the first method, the customers use the applications via an internet connection. There are several services with is used splay, such as Google Maps, YouTube. In the second method the user has got a large number of information that transfers to cloud. In the both method, the user's resources are resided on the cloud that is a potential tendency of regularity and legal issues.

3. The contractual issues

Cloud customer should be aware of its needs and restrictions to identify the legal barriers with cloud provider. It should be determined whether the provider meets their needs. There are some obligation that should be considered in contract and the provider must fulfill this obligations to protect the consumer's data.

3.1. Availability of service

Availability is the most important anxiety for cloud customers when they have deposited their data in cloud. In comparison with traditional systems, the risk of failure in accessibility for public clouds consumers, is relatively high. Additionally, the vulnerability in web browsers could increase the failures too.

3.2. Privacy

Cloud computing does not threaten the privacy, but outsourcing data into the cloud means that data could be out of direct control. Especially when the data are stored in the data centers outside of binderies. Cloud consumers should be aware of the security and privacy commitments specially in the case of transferring sensitive data. Without any assurance of privacy it's inappropriate to transfer the susceptible data into a cloud. To insuring data privacy, the contractual measures could be take into the account. Anything in term of privacy should be considered. The contract should guarantee that any act on cloud infrastructure do not affected the privacy of data.

The providers are unallowed to use the data for any individual purpose like advertising or other purposes and it must be mentioned in agreement. Cloud providers should ensure their customers of enforcing those agreements too.

3.3. Confidentiality

The information of cloud costumers should have an acceptable level of confidentiality. Especially when the cloud provider has access to sensitive data, the protection level should be more potent. To achieve this bourgeon, the provider should be aware of the level of data confidentiality to make the proper level of protection. It could be maintained in contract to restrict the access of provider's employees to data.

3.4. Provider's record

The cloud customers should have a list of provider's records to compare and choice the best one. In some countries there are a checklist of record management and the cloud which help users to refer it. Such checklists must be updated according to provider's activities.

3.5. Data recovery

The risk of losing data in some disasters or abuses is another important aspect in cloud security. In disasters like fire or in technical errors the data could be lost permanently. In a number of circumstances there are the risk of jobbery by provider's persons or external parties. To decrease this threats the provider should back them up. In their agreement the proper technical and mechanisms for recovery should be considered to address this problem. A compensation from the cloud provider should be considered in agreement to expiate in the loss of data as a result of knowingly or unknowingly negligence act. This responsibility could be more specific to recover the more sensitive and delicate customer's data.

3.6. Malicious codes

The nature of multi-tenant of cloud provides a potential opportunity for affecting the malicious codes. Therefore the customer should be sure that provider established sufficient protection policies against this kind of threats. Thus considering this type of risk and the countermeasures is essential.

3.7. Functionality

Customer‘s right of access may not provide the require degree for a full range of data. It means that it ‘s not able to access to meta data which is relevant to own data . It could be maintained in contract to extend the customer ability and permissions.

3.8. Integrity

Data integrity is critical for cloud providers. Data deterioration could happen at any data storage. Data decay could happen simply by migration to the other platform which is the nature of cloud. The cloud data center could be vulnerable to data deterioration. The customer could be ensure that every possible solution has been considered by provider to prevent data deterioration. The provider should provide the legal responsibility in the agreement. There are several way to check the integrity of data. Using the hash value and comparing with the backup hash value, programmatic checks, Spectra Logic, etc are the available method to ensure integrity (C. Marsh, 2013).

Conclusion

Cloud computing becomes a most important interest for many users and businesses. The logistical issue is steal a challenge of the customer's data. In this direction the legal issues are uncertain. The rights liability should be determined in contract for both customer and provider. Using these kind of arguments, assure the protection of data.

REFERENCES

A. Mohamed (2009). A History of Cloud Computing. (2010). from Computer Weekly: http://www.computerweekly.com/Articles/2009/03/27/235429/a-history-of-cloud-computing.htm

R. Capurro (2005). Privacy. An intercultural perspective. In *Ethics and Information Technology*, P 37–47.

A. Haeberlen (2010). A case for the accountable cloud. *SIGOPS Oper. Syst. Rev.* 44, 2, 52-57.

A. Cavoukian (2008). Privacy in the clouds. In Identity in Information Society (1) (2008) p. 89-108.

B Thompson, (2008). Storm Warning for Cloud Computing, available at
http://news.bbc.co.uk/2/hi/technology/7421099.stm (accessed 23 Mar 2009).

B Thompson,(2008). Storm Warning for Cloud Computing, available at
http://news.bbc.co.uk/2/hi/technology/7421099.stm (accessed 23 Mar 2009).

B. R Kandukuri and A. Rakshit (2009). Cloud Security Issues. In *Proceedings of the 2009 IEEE international Conference on Services Computing*, Washington.

C. Marsh, Data Integrity in theCloud (2013), Available: http://www.wwpi.com/, (21 Sep 2013).

C. Ess. (2008). Culture and Global Networks, Hope for a Global Ethics? In Information Technology and Moral Philosophy, Jeroen van den Hoven and John Weckert (Eds.). P 195-225.

D. Murley (2009). Law Libraries in the Cloud. Law Library Journal, Vol. 101, No. 2.

D. Mangot, (2009). EC2 Variability: The numbers revealed: Measuring EC2 systemperformance. http://tech.mangot.com/roller/dave/entry/ec2, Web page, Part of theseries urandom Mangot ideas.

D.A. Menascé and P. Ngo (2009). Understanding cloud computing: Experimentation andcapacity planning. In Computer Measurement Group Conference.

D. Miras et al (2002). A survey on network QoS needs of advanced internet applications.Working Document of Internet 2 QoS Working Group.

ENISA - The European Network and Information Security Agency (2009), Cloud Computing, Benefits, risks and recommendations for information security.

G. Collste (2007). Globalization, Ict-Ethics and Value Conflicts, In the ETHICOMP Journal (3).

Gartner (2009). Gartner Special Report, the What, Why and When of Cloud Computing, Available: http://www.cioupdate.com/features/article.php/3827971/The-Five-Attributes-of-Cloud Computing.htm (Oct 2012).

J. Fenn, M. Raskino and B. Gammage (2009). Hype Cycle for Emerging Technologies, (Retrieved 13.6.2010 Available: http://www.gartner.com/resources/169700/169747/gartners_hype_cycle_special__169747.pdf)

J. Van den Hoven (2008). Information Technology, Privacy and the Protection of Personal Data. Information Technology and Moral Philosophic, P 301-321.

J. M. Grimes, P. T. Jaeger and J. Lin (2009) Weathering the Storm: The Policy Implications of Cloud Computing.Available: http://nora.lis.uiuc.edu/images/iConferences/CloudAbstract13109FINAL.pdf (Sep 2013).

K.P. Andriole and R. Khorasani. (2010). Cloud Computing: What Is It and Could It Be Useful? Journal of the American College of Radiology. Volume 7, Issue 4, Pages 252-254.

L. Yao-Huai (2005). Privacy and Data Privacy Issues in Contemporary China. Ethics and Inf. Technol. 7, 1 , 7-15.

M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis and A. Vakali. (2009). Cloud Computing: Distributed Internet Computing for IT and Scientific Research. IEEE Internet Computing, vol. 13, no. 5, pp. 10-13.

M. R. Nelson (2009). The Cloud, the Crowd, and Public Policy. Issues in Science and Technology.

Moor, J. (2006). Why we need better ethics for emerging technologies. Ethics and Information Technology, 111-119.

P. Wolter and A. van Cleeff (2009).The Precautionary Principle in a World of Digital Dependencies. In Computer, vol. 42, no. 6, pp. 50-56.

P. Mell and T. Grance. The NIST definition of cloud computing. National Institute of
Standards and Technology, 2009.

R. C. Picker (2008). Competition and Privacy in Web 2.0 and the Cloud. U of Chicago Law & Economics, Olin Working Paper No. 414.

R. Gellman (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, World Privacy Forum.

S. Paquette, P.T. Jaeger, and S.C. Wilson (2010). Identifying the security risks associated with governmental use of cloud computing. Government Information Quarterly 27(3), pp. 245 - 253.

K. Won (2009). Cloud Computing: Today and Tomorrow. Journal of Object technology. Vol. 8, No. 1.

S. Paquette, P. T. Jaeger and S. C. Wilson (2010). Identifying the security risks associated with governmental use of cloud computing, Government Information Quarterly.

S. Pearson and A. Charlesworth (2009) Accountability as a Way Forward for Privacy Protection in the Cloud, In Cloud Computing, M.G. Jaatun, G. Zhao, and C. Rong (Eds.), p. 131–144.

Vaquero, L. M., Rodero-Meniro, L., Caceres, J., & Lindner, M. (2009). A Break in the Clouds: Towards a Cloud Definition. Computer Communication Review 39 (1), 50-55.