2018 • Issue 2

FACULTY OF LAW, UNIVERSITY OF MALAYA

CELEST

CENTRE FOR LAW AND ETHICS IN SCIENCE AND TECHNOLOGY





Does Your Personal Data Remain Private In The Cloud?

By Pardis Moslemzadeh Tehrani, PhD

Faculty of Law, University of Malaya

Author's Biography

Pardis Moslemzadeh Tehrani is a senior lecturer at the Faculty of Law, University of Malaya. Her research interests lie in the areas of cyberterrorism, cyberlaw, and international humanitarian law. Pardis's research has been widely published in peer-reviewed journals and she has presented papers at national and international level conferences. She is a member of the editorial review board in a number of journals. She is also an international scientific member of the Australian and New Zealand Society of International Law. Pardis's most recent book is Cyberterrorism: The Legal and Enforcement Issues (World Science and Imperial College Press of London, 2017).

eISSN 2637-031X

What is Cloud Computing?

Cloud computing is an Internet-based model of computing which provides software, applications, platform devices, data storage and other resources on 'a pay as you go' basis. The resources are accessible wherever Internet connections are available. Cloud computing technology provides users with computer resources which allow them to create scalable, flexible and cost-effective environments for development and hosting applications.

The US National Institute of Standards & Technology describes cloud computing as a platform that allows easy, on-demand network access to resources such as networks, servers, storage and applications that run under minimal intervention from service providers. [1] In simple terms, it is a storage service that merely requires an Internet connection.

Cloud computing often deals with personal and sensitive data of individuals or entities. Such data should be protected from any unlawful access and, accordingly, requires the highest level of privacy. Personal data may be defined as personally identifiable information that could potentially identify a specific individual. It may also be defined as any information that can be used to distinguish one person from another. [2]

Cloud federation is the practice of interconnecting the cloud computing environments of two or more service providers. As the cloud federation involves a substantial number of groups working together to provide services, a large amount of personal data exchanges occur in the cloud. [3] Accordingly, it is important to ensure the privacy of the personal data by shielding it from any unlawful access.

...cloud computing as a platform that allows easy, on-demand network access to resources such as networks, servers, storage and applications...often deals with personal and sensitive data of individuals or entities.

Privacy Risks in Cloud Computing

The notion of 'privacy' in relation to personal data is not confined to confidentiality but extends to the right to control how that data is communicated. As noted in the International Telecommunication Union's Technology Watch Report, 'privacy' encompasses "the right to self-determination, that is, the right of individuals to 'know what is known about them', be aware of stored information about them, control how that information is communicated and prevent its abuse." [4]

There are different types of threats to privacy in cloud computing. A type of threat concerns the unauthorized access to data stored in the cloud by cloud attackers. The two main types of attackers in the cloud infrastructure are internal and external attackers. Internal attackers are often employees of the cloud service provider or third party providers that support the operation of the cloud service. [5] They are usually given the authorisation to access the database in the cloud. However, they abuse such authorisation, whether to achieve their personal interest or to support a third party, by executing attacks on the confidentiality, integrity, and availability of information within the cloud service. [6] An example of such an attacker is the cloud service providers themselves who access the personal data of their customers for their own benefit or profit.

Most service providers monitor the personal data of their customers in order to create personalised advertisements which deliver individualised content that is targeted to meet the recipients' needs or interests.

Most service providers monitor the personal data of their customers in order to create personalised advertisements which deliver individualised content that is targeted to meet the recipients' needs or interests. Complex data and statistics are recorded, bundled and analysed to facilitate user profile marketing and make predictions on what a user might buy in the near future. [7]

Governments also often fall within this category of cloud attackers. [8] Governments have the authority to access the data in the cloud to protect national security and fight against terrorism. This may be seen in cloud forensic cases which involve digital investigation in the cloud computing environment. In fact, it is said that the migration of data from a suspect's hard disk to the cloud presents an opportunity to the Government to covertly investigate a wide range of data; this obviates the need to conduct physical searches of computers which may alert suspects that they are being investigated. [9] It has also been suggested that Governments have the authority to compel cloud service providers to de-encrypt and encrypt cloud-based data for them. [10]

Many IT managers fear that they will put their data at risk by moving their data to the cloud because they are unsure that the data will be protected from Government interception. Since the cloud service provider is legally obliged to provide access to the Government when required to do so, there is limited privacy in the cloud environment. [11] In a decision by the US Court of Appeals for the Second Circuit, Microsoft Corp v United States, [12] the court held that the Government could not compel Internet Service Providers to turn over data that are stored overseas, even with a warrant.

However, the case revolved around the extraterritorial application of the US statute known as the Stored Communications Act and the court did not address the issue of data placed within a country.

The second type of attackers, that is, external attackers mainly comprise hackers who access cloud users' confidential data for illegal activities. This can include credit card information, bank details, private and confidential documents, and health records. Many companies are subject to external attacks which, if successful, allow third parties to access the personal and financial information of individuals. [13]

Other than the above, the lack of control over the lifecycle of one's personal data stored in the cloud also poses privacy risks. [14] When a cloud customer erases personal data from his cloud, he will want assurance that the cloud provider does not have a copy of the erased data. [15] If there is indeed a copy of the erased data, which is often the case, then the act of erasing is redundant. This shows that cloud customers have no control over the lifecycle of their personal data as most data are completely erased only when they change the service provider. [16]

There are also security concerns in regard to the backing-up of data by cloud service providers. Data backup is critical for businesses to recover their data in case of system failure. However, since backing-up of data is usually done without the explicit consent of the relevant parties, there is concern about possible leakages of the backed-up data. The concerns regarding security are heightened because the location of the data is not known to the cloud customers. [17]

Addressing Privacy Challenges in the Cloud

Cloud computing is a new technology and as new technology is invariably ahead of the law, the risk of breaches to data privacy in the cloud is an area which the law has to grapple with today. This is further complicated by the different cloud computing structures that are available and which give rise to different privacy concerns.

One means of ensuring data privacy is to maintain an appropriate level of data protection. Although data protection measures will not always be able to safeguard data privacy, it can resolve many data privacy issues. However, there are different types and standards of data protection and they vary according to different countries. There are many approaches available in protecting privacy and this wide spectrum can be seen in the range and levels of protection that vary from one country to another. The European Union is said to have one of the most comprehensive sets of data protection rules with laws enacted specifically for that purpose. This can be seen both in the previous directive and also in the new and improved regulations.

The diversity of services and the various access requirements of domains in cloud computing models require proper access control policies. [18] It is important that access control services integrate privacy-protection requirements through rules and, at the same time, capture the relevant aspects of Service Level Agreements (SLA). [19] Cloud models also need to have a proper storage of users' accounts to protect privacy since clients may not be willing to allow a provider to store their detailed accounting records other than for billing purposes.

Hence, the use of privacy-aware framework for access control and accounting services and implementing compliance checking can to some extent allay the fears of cloud users. [20]

The cloud computing environment has six specific areas which require substantial security. These are data at rest, data in transit, authentication of users, separation among customers, cloud legal and regulatory issues, and incident response. A cryptographic encryption mechanism is the best option for securing data at rest and data in transit. Encrypted data normally involves converting or transforming specific personal data by applying an algorithm or a key to ensure its security is heightened.

...since backing-up of data is usually done without the explicit consent of the relevant parties, there is concern about possible leakages of the backed-up data. The concerns regarding security are heightened because the location of the data is not known to the cloud customers.

Authentication and integrity protection mechanisms ensure that data is relayed where the customer wants it to be relayed and is not modified in transit. Having a strong authentication system is extremely important for cloud providers. Cloud providers with a strong identity management system receive notifications in real-time when a user's access privilege is assigned or revoked, and this allows the providers to modify the user's cloud access within a very short span of time.

With respect to the separation between cloud customers, there is a need to avoid intentional access to sensitive data. For this purpose, the providers would normally use virtual machines. In case of a security breach in a cloud provider, an automated notification is the best solution as it allows customers enough time to take the necessary action.

Lastly, to deal with privacy issues in a cloud computing environment, the customer's legal experts need to examine the provider's policies, regulations, and practices as well as the SLA to ensure its adequacy and to verify that it encompasses all the legal and technical aspects. Data security and export, compliance, auditing, data retention and destruction, and legal discovery are other additional issues which need to be considered by the customers to ensure that an adequate level of protection is given by the service providers and avoid any possible losses. [21]

References

1. P. Mell & T. Grance. 'The NIST Definition of Cloud Computing Recommendations of The National Insitute of Standards and Technology' available at http://faculty.winthrop.edu/domanm/csci411/Handouts/NST.pdf/. Accessed on 20 September 2018.

2. M. Rouse, 'Personally Identifiable Information (PII)' available at http://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information/. Accessed on 20 September 2018.

3. This is for the purpose of load-balancing traffic and accommodating spikes in demand, available at https://searchtelecom.techtarget.com/definition/cloud-federation/. Accessed on 20 September 2018.

4. ITU-T Technology Watch Report, 'Privacy in Cloud Computing', March 2012 available at https://www.itu.int/dms_pub/itu-available at t/oth/0B/15/T0B150000123301PDFE.pdf/. Accessed on 20 September 2018.

5. Ibid.

6. T.TagElsir A. Osman & A. babiker A/Nabi Mustafa, 'Internal & External Attacks in cloud computing Environment from confidentiality, integrity and availability points of view' IOSR Journal of Computer Engineering (IOSR-JCE) (2015) 17 (2), 93-96 available at http://www.iosrjournals.org/iosr-jce/papers/Vol17-issue2/Version-5/N017259396.pdf/. Accessed on 20 September 2018.

7. K. Harika, B. Dada Khalande & G. Rama Subba Reddy, 'Aggregate Recommendation and Effective Query Services in The Cloud with Data Perturbation' International Journal of Science Technology and Management (2015) 4 (7), 78-82.

8. A. Adrian, 'How Much Privacy Do Clouds Provide? An Australian Perspective' Computer Law & Security Review (2013) 29 (1), 48–57.

9. K. Bert-Jaap, M. Goodwin, 'Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law' (2014) Tilburg Institute for Law, Technology, and Society, CTLD – Center for Transboundary Legal Development.

10. Ibid.

11. S. Kar , Fears of Government and Legal Intervention Slows Cloud Adoption available at http://cloudtimes.org/2013/02/16/fears-of-government-and-legal-intervention-slows-cloud-adoption/. Accessed on 20 September 2018.

12. Microsoft Corp. v. United States 829 F.3d 197 (2d Cir. 2016).

13. R. H. Weber, 'The Digital Future – A Challenge for Privacy?' Computer Law & Security Review (2015) 31 (2), 234-242.

14. S. Pearson & A. Benameur, 'Privacy, Security and Trust Issues Arising from Cloud Computing' 2nd IEEE International Conference on Cloud Computing Technology and Science (2010), Indianapolis, IN, USA. IEEE publisher available at http://barbie.uta.edu/~hdfeng/CloudComputing/cc/cc05.pdf/. Accessed on 20 September 2018.

15. Ibid.

16. Ibid.

17. J. Sen, 'Security and Privacy Issues in Cloud Computing' 3rd International Conference on Computing for Sustainable Global Development (2016) available at https://pdfs.semanticscholar.org/4dc3/70d253020947a8e66b701e12dd0233161229.pdf/. Accessed on 21 on September 2018.

18. An access control system is a collection of components and methods that determine the correct admission to activities by legitimate users based upon preconfigured access permissions and privileges outlined in the access security policy.

19. SLA is a part of a service contract between the consumer and provider that formally defines the level of service.

20. H. Takabi & J. B.D, Joshi, 'Security and Privacy Challenges in Cloud Computing Environments' IEEE Security & Privacy, The IEEE Computer and Reliability Societies (2010) available at http://csis.pace.edu/~marchese/SE765/Paper/security2.pdf/. Accessed o 20 September 2018.

21. J. Sen, Security and Privacy Issues in Cloud Computing, Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA available at https://www.researchgate.net/publication/305380675_Security_and_Privacy_Issues_in_Cloud_Computing/. Accessed on 3 October 2018.

Editor: Dr Kalavathy Maruthavanar
Production Editor: Dr Mohammad Firdaus Bin Abdul Aziz