The problem of binary distinction in cloud computing and the necessity for a different approach: Positions of the European Union and Canada

Pardis Moslemzadeh Tehrani *, Johan Shamsuddin Bin Hj Sabaruddin, Dhiviya A.P. Ramanathan
Faculty of Law, University of Malaya, Malaysia

Abstract
The development of Cloud Computing is an undisputable fact that is present in this modern era. It is a widely used system, which consists of users from ordinary individuals to multinational companies. However, despite its benefits, there is a problem of accountability in Cloud Computing. Accountability is vital for the allocation of responsibility to ensure the non-existence of threats concerning privacy and security of personal data stored in a Cloud. Both these issues are interconnected because one will not be able to exercise the principle of accountability by omitting the allocation of responsibility. Due to the complexity of the Cloud Computing infrastructure, the line in the distinguishing the role of controller and processor is blurred. This article serves to provide a better understanding of the role of Cloud Computing as well as to configure the need for either a modified or a completely different approach. Furthermore, this article will discuss the different approaches whilst providing a detailed analysis of the roles of the controller and processor. Clear and unambiguous roles and responsibilities will help to reinforce the principle of accountability. This article will compare the positions of Canada and the European Union, because the Canadian approach provides a different outlook since they do not follow the same binary distinction concept in allocating responsibility for controller and processor. This discussion hopes to bring awareness for the discrepancies in the current system and attempts to recommend a possible outcome to curb the problems relevant to this issue.

Keywords:
Cloud Computing
Controller
Processor
Accountability
Cloud service provider
Allocating responsibility

© 2017 Pardis Moslemzadeh Tehrani, Johan Shamsuddin Bin Hj Sabaruddin, Dhiviya AP Ramanathan. Published by Elsevier Ltd. All rights reserved.

* Corresponding author. Faculty of Law, University of Malaya, Jalan Universiti, 50603 Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur, Malaysia.
E-mail address: pardismoslemzadeh@um.edu.my (P.M. Tehrani)
http://dx.doi.org/10.1016/j.clsr.2017.03.014
0267-3649/© 2017 Pardis Moslemzadeh Tehrani, Johan Shamsuddin Bin Hj Sabaruddin, Dhiviya AP Ramanathan. Published by Elsevier Ltd. All rights reserved.
1. Introduction

Cloud, also known as a visible mass of condensed water vapour floating in the atmosphere, is typically known for being high above the ground. We often symbolize cloud in mind maps as the top of the chart followed by subsequent details. In such a mind map, the column with the cloud is the largest fact and all that falls below it are merely subsections of what follows the cloud. Cloud Computing is also derived from a similar concept. Cloud Computing is an Internet based system where virtual software provides software, infrastructure, platform devices and other resources and hosting to another customer on a pay as you go basis. Cloud computing allows users to focus less on how to manage the resource and more on their core business processes. To explain, the managing and monitoring aspects of data storage are handled within the cloud computing by the cloud service providers themselves. Cloud Computing reduces costs and has the potential to transform a data center from a capital-intensive set up to a variable priced environment.

Nevertheless, the Cloud Infrastructure is diverse in nature, ranges from lucrative, and mission critical business functions to sensitive information and expressive content. Because of the nature of data that is being dealt with, there is a considerable amount of potential dispute that can arise. One concern is the privacy of the end user. This is of paramount importance because Cloud Computing infrastructure contains sensitive data of the end user, which requires heightened security. One example is where the government wiretaps the personal data in Cloud for surveillance. There are instances where the service provider provides the FBI wholesale access to its network, enabling agents to tap customers’ data at will without obtaining permission of the person in charge. This is a clear breach in the general expectation of privacy of the individual who stored their personal data in the cloud services because there is room for illegal wiretapping. Babak Pasdar, current CEO of New York-based Bat Blue, has said that it is alarming how this carrier ended up embracing wiretapping.

2. Cloud Computing

The National Institutes of Standards & Technology (NIST), which has formulated a universally adopted definition, describes cloud computing as a platform that allows easy, on-demand network access to resources such as networks, servers, storage, applications and other virtualized resources. In contrast to traditional computing platforms, access to such platforms is achieved through the Internet and is paid for on a per-use basis. Cloud Computing is also derived from a similar concept. Cloud Computing Recommendations of the National Institute of Standards and Technologyhttp://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf accessed 26 December 2016, p.2.
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات