What is Hidden Within the Cloud?

Aikaterini Gkritsi
Electronics and Computer Science
University of Southampton
ag2006@soton.ac.uk

Abstract

Over the past few years cloud computing has become one of the most significant technological trends. The aim of this paper is to discuss the main characteristics of cloud computing, identify the challenges concerning the security and control of information within the cloud and finally to examine how secure information can be in it. Section one gives an overview of the technology by presenting its key aspects and architecture. The security issues about its adoption are explored briefly in section two followed by possible ways to prevent these threats on section three. Finally, in section four the research focuses on the future of cloud computing and closes with an evaluation of how secure the cloud is on section five.

1. Introduction

Lately more and more enterprises tend to shift to cloud computing because as the president of Hewlett-Packard Russ Daniels says, it minimises the cost of information technology, but it is not only that. It allows customers to avoid the expense and hassle of having to install and maintain applications locally [1].

Cloud computing can formally be defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[1] or more simply, it is the ability to access files, data and services hosted by another party using a browser and be charged only for the computing services used [2].

This technology is usually confused with grid and distributed computing. As Aymerich *et al.* state, "each cloud is managed by a computational grid, but the reverse is not true, i.e. a grid is unable to also implement cloud computing technologies" [3].

1.1. Architecture

The cloud has a four-layer architecture and it consists of the *application, platform, unified resource* and *fabric layer* [4]. The lowest level of the architecture is the *fabric layer, which* represents the different devices with which users may have access to the Internet. Then comes the *unified resource layer* which contains abstracted resources that can be represented to the end user e.g. a file or a database system and then the *platform layer* which offers a deployment platform. Finally, at the top level there is the *application layer*, which contains applications capable to access the cloud [4] (Figure 1).

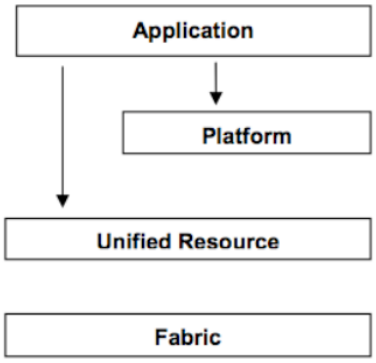

Figure 1: Architecture of cloud computing

Furthermore, cloud computing accommodates a number of different models [5] such as the *Infrastructure as a Service (IaaS), Platform as a Service (PaaS)* and finally *Software as a Service (SaaS)*. Each of these models is responsible of the level of control over the management of the computing

[1] Mell, T. & Grance, T., "The NIST Definition of Cloud

infrastructure and the specification of responsibilities for managing its security [2] (Figure 2).

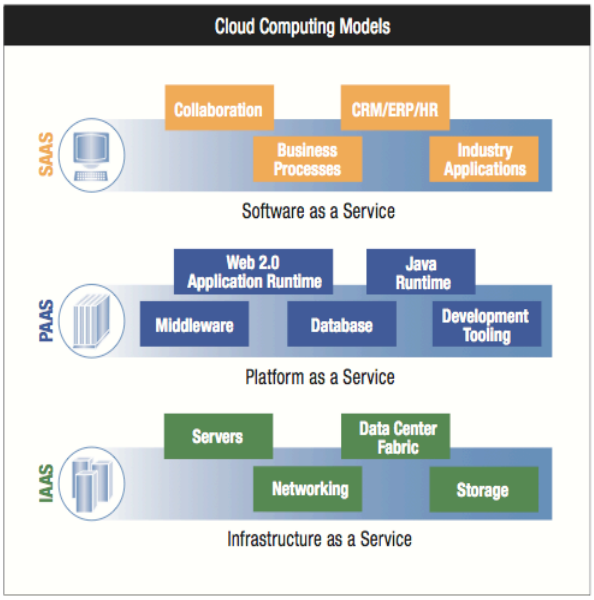

Figure 2: Cloud computing models

Specifically, in IaaS model, cloud vendors offer hardware and computing power to clients on an as-needed basis[3] e.g. Amazon's EC2 and Tycoon [5]. In SaaS, the provider is in charge of the security management of the cloud but offers some responsibility to the client of managing the resources. In this case, cloud providers offer software applications over the Internet, therefore customers do not have to purchase the software and they avoid the responsibility of having to upgrade and maintain the software e.g. Google Docs and Microsoft Office Live [5]. Moreover, PaaS offer even more control to the client in terms of managing and configuring the resources. Here, vendors provide applications which are necessary to build other applications and offer services from the Internet, without having to download or install any software. PaaS services also provide applications to support the entire development lifecycle[3]. However, there is lack of interoperability between providers so another vendor may not support a specific application or the customer may need to pay a high fee to do so [11] e.g. Microsoft's Azure or Google's App Engine [5].

Finally, there are three different types of clouds, the *private*, the *public* and the *hybrid cloud*. The difference between these types lie on where the cloud is hosted, whether it is run from the customer or the cloud provider, and if it is a shared or private infrastructure. In particular, public cloud is a "stand-alone"[4] or proprietary cloud, which is available for public use and managed entirely by the provider. Private is the cloud which is built to be operated solely by the user. This type of cloud is usually designed by the IT department of the customer[4] and is managed either from the customer or the service provider. Last by not least, hybrid cloud is a combination of private and public clouds and it provided in-house and external hardware and software resources. It provides scalability and low cost as public clouds but it is more secure and contains all the software necessary for the client, as a private cloud[4].

1.2. Advantages and Challenges

Cisco supports that cloud computing fundamentally changes the way that IT services are delivered to enterprises[4]. First, it reduces the cost since customers pay only by consumption and avoid the cost of hardware maintenance and storage capability; it is very scalable and highly available. It also provides application and integration support as well as flexibility on mitigating or relocating workload[4]. Through the cloud, users have access to large computing power that otherwise would not be affordable especially for individual users or start up companies, allowing real-time collaboration and remote access [3]. Furthermore, the cloud has dynamic infrastructure [1] because it is easier to deal with "peak load situations" without the need of additional hardware since the cloud offers on-demand resources [3]. Finally, the use of SOAP (Simple Object Access Protocol), WSDL (Web Service Description Language) and XML-based protocols, facilitate the interaction legacy resources and other infrastructure services [1].

However, there are some doubts concerning its adoption mostly because of the fear of losing control over the data and computing resources since it is no longer stored locally. Cloud computing supports different kinds of models; therefore it is difficult to guarantee the security of resources and to specify the

[2] IBM Point of View: Security and Cloud Computing", http://www.ibm.com/common/ssi/fcgi-bin/ssialias?infotype=SA&subtype=WH&appname=SWGE_TI_SE_USEN&htmlfid=TIW14045USEN&attachment=TIW14045USEN_HR.PDF, [Accessed: October 2010]

[3] Motahari-Nezhad, H. R., Stephenson, B. & Singhal, S., "Outsourcing Business to Cloud Computing Services: Opportunities and Challenges" http://www.hpl.hp.com/techreports/2009/HPL-2009-23.html, [Accessed: October 2010]

[4] Cisco, "Cisco Cloud Computing – Data Center Strategy, Architecture, and Solutions", http://pdfebooksfreedownload.com/story/cisco-cloud-computing-%E2%80%93-data-center-strategy-architecture-and-solutions/, [Accessed: October 2010]

responsibilities of the client and the provider for each of these models. There are also doubts because of latency and bandwidth related issues as well as vendor "lock-in" and the lack of interoperability of applications between providers because of lack of standardisation.

2. Security Issues

The most common fear on using the cloud is the lack of control and transparency of the data because it is managed from a third party and not from the client itself, therefore many enterprises tend to put only their less sensitive data in the cloud [6]. There are also some attacks caused by malware injection attacks, cloud spoofing and flooding attacks due to direct or indirect Denial of Service (DoS) [7]. Additionally, there are authentication and authorisation issues because the authorisation and authentication frameworks of the client do not apply on the cloud so they cannot apply their own security metrics and policies on the data stored in the cloud [6]. Also, providers deliver services by sharing infrastructure but the underlying infrastructure of these components was not designed to offer isolation for multi-user architectures so this allows attackers to gain unauthorised access[5]. Last but not least, users hesitate to adopt cloud computing because they are concerned about the location of their data, its recovery in case of a disaster or bankruptcy of the provider, segregation of the data since the cloud is a "shared environment alongside data from the customers [8] as well as the availability of services e.g. outage of Gmail on 2008[5].

3. How secure can it get?

There has been a lot of discussion on how to make the cloud more secure. In particular, some state that 100% availability; security and privacy protection within the cloud is impossible [2]. Some of the solutions that have been suggested are the application of a scheme that ensures the correctness of user data within the cloud and identifies the misbehaving server(s) [9]. Others suggest that in order to protect against potential threats both customers and providers should take action and make use of SLA (Service Licence Agreement) which defines the responsibilities of both the client and the provider and helps on issues such as the identification of customer's needs, identification of unrealistic expectations and demands from the user, availability etc. [8]. IBM suggests that "characteristics of clouds such as standardisation, automaton and increased visibility into the infrastructure can dramatically boost the security levels" within the cloud [2] but for this to happen, access control policies should be established as well as encryption of data in motion and in rest[2].Lastly, since the data stored in the cloud is both client's and provider's responsibility, businesses should make use of hybrid clouds instead of public[2] and vendors should avoid centralisation of data and aim for their compartmentalisation[4] as well as encrypting data with for example searchable, predicate, homomorphic or Private Information Retrieval (PIR) [6] encryption.

4. Future

There is a belief that with the current economic crisis many enterprises will swift to cloud computing [1]. Currently, companies like Intel, Yahoo and HP Labs develop services like dynamic clouds and cloud-computing-specific chips. Additionally, IBM Research released the Research Compute Cloud, which is "an on-demand globally accessible set of computing resources that support business processes" [1]. Cisco envisions the use of cloud computing as "a phased infrastructure build-out of the cloud industry" that will change the way that IT resources are used[4]. Moreover, cloud integration services will be developed to fulfil the need of integrating applications and data from different clouds and that ecosystems of clouds will be formatted and probably users will shift towards hybrid systems that promise better availability and security [2]. Since 2008, about 69% of Americans and nearly 1,500 companies in India shifted into cloud computing [10]. Finally, the US government projects that between 2010-2015 the spending on cloud computing will be about the 40% of the compound annual growth rate and will excess $7 billion by 2015 [10].

5. Conclusion

This paper described the architecture and characteristics of cloud computing and its aim was to investigate the security issues around the subject and identify possible solutions in order to evaluate whether it is safe store data within the cloud or not. Judging from all the benefits that a client may have using the cloud and the future trends on cloud computing adoption it is obvious that cloud computing is a very promising technology. Even though there are some security issues concerning the control of data in the cloud and DoS attacks that hold back its adoption, it was shown that there are several ways of dealing with

[5] Top Threats to Cloud Computing, http://www.cloudsecurityalliance.org/topthreats.html

them. Currently, storing data in the cloud is slightly risky but if both clients and providers try to implement and adopt the suggestions on how to make the cloud more secure, storing data into the cloud will become much more secure that it is today.

6. References

[1] Levitt, N., *Is Cloud Computing Really Ready for Prime Time?* Computer, vol. 42, no. 1, pp. 15-20, Jan. 2009

[2] Kim, W., "Cloud Computing: Today and Tomorrow"*, ournal of Object Technology,* vol. 8, no. 1, January-February 2009, pp. 65-72

[3] Aymerich, F.M., Fenu, G. & Surcis, S., "An Approach to a Cloud Computing Network"*, ICADIWT 2008: First International Conference on the Information and Web Technologies, 2008,* vol., no., pp.113-118, 4-6 Aug. 2008

[4] Foster, I., Zhao, Y., Raicu, I. & Lu, S., "Cloud Computing and Grid Computing 360 – Degree Compared"*, GCE '08: Grid Computing Environments Workshop, 2008,* vol., no., pp.1-10, 12-16 Nov. 2008

[5] Lenk, A., Klems, M., Nimis, J. & Tai, S., "What's Inside the Cloud? An Architectural Map of the Cloud Landscape", *ICSE Workshop on Software Engineering Challenges of Cloud Computing, 2009* vol., no., pp.23-31, 23-23 May 2009

[6] Chow, R., Golle, P., Jakobsson, M, Masuoka, R. & Molina, J., "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", CCSW 2009: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, 2009 November 13, Chicago, IL. NY: ACM, 2009, 85-90

[7] Jensen, M, Schwenk, J., Gruschka, N. & Iacono L. L., "On Technical Security Issues in Cloud Computing", *International Conference on Cloud Computing, IEEE, 2009* vol., no., pp.109-116, 21-25 Sept. 2009

[8] Kandukuri, B. R., Paturi, R. V. & Rakshit, A. "Cloud Security Issues"*, SCC '09: International Conference on Services Computing, IEEE, 2009,* vol., no., pp.517-520, 21-25 Sept. 2009

[9] Wang, C., Wang, Q., Ren, K. & Lou, W. "Ensuring Data Storage Security in Cloud Computing" *IWQoS: 17th International Workshop on Quality of Service, 2009,* vol., no., pp.1-9, 13-15 July 2009

[10] Kaufman, L.M.; , "Data Security in the World of Cloud Computing," *Security & Privacy, IEEE* , vol.7, no.4, pp.61-64, July-Aug. 2009

[11] Velte, T., Velte, A. & Elsepeter R. C., "*Cloud Computing: A Practical Approach",* The Mc-Graw-Hill Companies, USA, 2010