Oct 28th, 9:00 AM - Oct 30th, 5:00 PM

Cloud Computing and Enterprise Data Reliability

Luan Gashi
University for Business and Technology, luan.gashi@ubt-uni.net

Cloud Computing and Enterprise Data Reliability

Luan Gashi

UBT – Higher Education Institution, Lagjja Kalabria, 10000 p.n.,
Prishtine, Kosovo
luan.gashi@ubt-uni.net

Abstract. Cloud services offer many benefits from information and communication technology that to be credible must first be secured. To use the potential of cloud computing, data is transferred, processed and stored in the infrastructures of these service providers. This indicates that the owners of data, particularly enterprises, have puzzled when storing their data is done outside the scope of their control.

Research conducted on this topic show how this should be addressed unequivocally. The provided information on the organization of cloud computing models, services and standards, with a focus on security aspects in protecting enterprise data where emphasis shows how data access is treated with reliability from providers of these services.

The topic turns to key security issues that companies should consider when they select the cloud service provider. Case studies from this research gives the fulfillment of these key security points from the providers of these services.

Keywords: AWS, EC2, IaaS, IEEE, ISO, NIST, PaaS, SaaS, SAS, SLA, SSL, TLS

1. Introduction

Cloud computing is a summary term for a group of techniques of advanced information technology. This grouping or technological development has changed the way information technology services are offered, accessed and paid. Some of the technology supporting these services are used long ago, but the combination of some of the most developed have enabled a completely new way of using IT.

The definition of cloud computing is something that is still being developed. According to the US National Institute of Standards and Technology (NIST) definition of cloud computing is [1]:

Cloud computing is a model that enables adaptability and access as needed in a group to share computer resources (eg computer networks, servers, landfill applications and other services) with which easily equip or released with minimal management or labor intervention service providers.

Like the majority of all new technologies, the development of which focus only on their functioning, as well as cloud computing, first the momentum of its development has the functionality and variety

of services offered by raising many questions on security aspects and control of these services. This indicates that users who tend the selection of providers of these services, consider the reliability in storing their data before to take them to the cloud.

There is a lack of knowledge on how to treat cloud computing in general reliability in storage, processing and transmission of data at the premises of companies that offer cloud services.

The purpose of this topic is to provide key security points which clarify the credibility of enterprises in storing their data in the cloud. This makes eased doubts or suspicions regarding the use of cloud computing by individuals or/and enterprises.

1.1. Operation and services to cloud computing

One of the terms that most often occurs in cloud infrastructure is the term "virtual" ie "virtualization". This term is used because in the infrastructure you can not physically access the device which are used as these devices and complete infrastructure are raised on platforms of programs that manage the hardware resources such as those of producers VMvare, Microsoft Hyper- V or Citrix offering from a physical unit some virtual services, platforms or infrastructure as virtualized, where the dealing in use by individuals or companies in the form of services for a fee which is usually calculated based on the time for which are used virtual devices or services. For this reason, often cloud computing is defined as service on "pay-as exploits" (*Pay as you go).*One form of these services are those called Web services which are found as the origin in the development of technology. These are based on cloud infrastructure, but the cost of their development and possession has been and remains up taking too long to implement despite the cloud computing which change completely this by incorporating virtualization technology that enables physical infrastructure to be used better and with much lower cost compared to the old way of these engineering services. Thus, according to NIST's (National Institute of Standards and Technology) all cloud services are categorized according to what is offered in three main categories, which are: infrastructure, platform and software.

1.2. Infrastructure as a service (IaaS)

Often individuals or enterprises must buy infrastructure which are not used frequently and have to spend thousands of euros to get the service they need, while companies offering cloud services is able to significantly reduce these costs by offering virtual infrastructure against a temporary acquisition or by use where the payment would be calculated on the basis of the hardware resource utilization; use time based on processors, memory, network dumps or use courier. The service provider in this case provides a virtual basic platform with a limited number of standard services such as storage, categorization, security and management of virtual appliances. Enterprises that use this kind of offer, can build infrastructures which provide services of high quality and expensive infrastructure of information technology towards a low price thanks to the cloud computing service, infrastructure as a service respectively. [3] [4] These virtual appliances can be named and configured as desired and access to them is done remotely using standard applications used for remotely access. They called virtual devices since the buyer does not buy the physical

device and does not have it, but it takes a fee for use of the agreed time of use. Some of the most popular companies that provide infrastructure as a service are: Amazon EC2, Microsoft Azure, Cloud.com, Rackspace.com and GoGrid.

1.3. Platform as a service (PaaS)

As provided infrastructure as a service, the same can also be provided as a service platform, but in this case the buyer or user shall not use the virtual device but gets to use a specific software platform. Platform as a service enables the use of different software by reducing the cost of software engineering, thus eliminates the need of development and marketing as well as reduce the risk and cost of building a software.

So, as a service platform is designed for developers who develop applications and distribute them in the same cloud computing environments. This platform also facilitates the work of the developers because they have nothing to deal with system upgrades and maintenance. Platform as a service enables developers to develop their applications without knowing anything about the infrastructure of the system. Examples of this platform are Google and Facebook. Users can use the Google API's to develop their applications, while Facebook allows users to write their own applications [3] [4].

Examples of companies that offer platform as a service are: Google App Engine, Amazon AWS, Microsoft Azure, SalesForce, etc.

1.4. Software as a service (SaaS)

The most important service of cloud computing is definitely the software which is known as software as a service since it is the part that has to do directly with service users and their applications. This has nothing to do with the software through which is offered cloud computing because often this confused it, but has to do with the software that created by developers in order to meet the requirements of different users, be they client or only user of the computer. Software as a service means the software which is based on a code that serves many users. This code aims to preserve the authorship of the software and the changes that can be made, but usually an option for users to adapt it to their needs. These software are developed and deployed in the cloud by service providers and may be accessed via the Internet, ie remote computer networks. The fee is based on the monthly payment mode or by use. By use of this service, customers reduce infrastructure maintenance costs for information technology like upgrades and software costs. Since these software can be accessed remotely, installing them is easy and there is no need to add hardware. Typical examples of such software are Webmail and Google Document.

With software as service (SaaS) cloud users subscribe via an application that is enabled by the cloud service provider includes the use of the software subscription, support, data storage and other services. The service provider is responsible for the management and maintenance of the basic platform and applications on which the service is provided, so users do not meet these responsibilities. Most renowned providers of these services are Google and Microsoft. While examples of software offered as a service are: SalesForce, Google Apps, Microsoft Office 365 and NetSuite. [4] [5]

1.5. Other types of service (XaaService)

It is important to note that services such as IaaS, PaaS and SaaS are three main categories of cloud computing services. Other types or as often referred to as everything as a service, to cloud computing services providing other means of information technology through it are referred like hybrid cloud services and are usually referring to the combination of three major cloud services. This type of service is usually identified as a special service in the cloud and based on this also takes appropriate name. [7] Among the best known of this group of cloud computing services are:

DAAS (*Database as a Service).* - Data base systems provide an interface through which data are accessed and managed. When this type of service is offered in the cloud it is also known as base data as a service. This type of service is quite usable and many businesses and applications based finance in reaching the use of this service.[8]

Naas (*Network as a Service).* - With the network as a service from companies offering cloud computing services is offered virtualized computer networks [9].

CAAS (*Communication as a Service).* - Communication as a service allows customers to use services like VoIP, VPN, PBX and unified communication without the cost of investment for setting up, hosting and management of related IT infrastructure as this remains the responsibility of providers. This includes maintenance for this service [10].

IPMaaS (*Identity and Policy Management as a Service).* - In this service, the companies offering cloud computing services, provide protection and security of access to the services published on the Internet. Companies that offer this service are over eliminating or at least amortization of attacks that can occur in terms of web publications or infrastructure to the IT for their clients.[11]

HPCaaS (*High Performance Computing as-a-Service).* - It is a new service that has been offered as a separate service in the cloud to the demands of users for super computers (high performance computers).[12] This processing power which can be powered together by millions of computers through special software and is offered apportioned to several personal computers used in parallel and working as if they were all in one.[7] [8]

1.6. Implementation models to cloud computing

Implementation models to cloud computing are found depending on the needs and requirements of users in dealing with the organization of infrastructure and its implementation in the cloud. Specifically, the most common models that are found are:

- Public Cloud
- Private Cloud
- Hybrid Cloud

2. Problem statement

When we talk about security in computer systems, immediately we think about what should be safe and who will provide it. An asset has a value implicit or explicit, and the higher this value is, the higher should be guaranteed safety. What is new in information technology are environments in which data and mechanisms for their protection and which have changed significantly compared with traditional ones. In cloud computing environments and data protection mechanisms are not under the control directly to the holders thereof.

A generalized approach that classifies assets and computer networks in the field of security, defines three main objectives that users should consider when dealing with the preservation of their data which are: confidentiality, integrity and availability. The concepts described below will be used as reference points for the problem which will be discussed in this paper and which therefore has to do with the reliability of data storage in cloud computing.

2.1. Limitations of control in cloud computing

The application of security controls in cloud computing is not the same as in traditional computing as in cloud computing environments may have different restrictions. These restrictions affect the application of security controls which may also depend on the establishment of information systems and the inherited system and control of its type.

2.2. Restrictions related to access

An important distinction that interfaces with access to information systems is the difference between access from external networks and internal computer. If the infrastructure that is used to access the information system is not under the control of the owner of the system, the security of transmissions through this infrastructure may not be so guaranteed. This kind of approach to type of access from external networks and information systems.
The key issues of information security to *cloud* computing is support for encryption of data and if the infrastructures of enterprise organizations are under the control of the holder of the information or not. This leads to liaise with restrictions on access
according to whether *cloud* service accessed by a network of external computer, and encryption of data is not supported, then this approach definitely limited by the low level of security and public system access where the reliability of data It is not guaranteed. [13]

2.3. Limitations of confidence in safety

Although reliability and confidence in most of the literature used in the same sense, they are not the same in terms of the implementation of information security systems. The difference between the reliability of a system and confidence in a system defines reliability as a type of insurance that a person or organization needs to have a system because there is simply no alternative.[13] When storage of data outside the enterprise and cloud computing made possible as the technology for premises computer, this technology needed to prove its credibility as an alternative offered for choice by

individuals or organizations in data storage or hosting their system of information.In cloud computing environments that are outside the scope of the data holder, the degree of control to the organization that cloud service providers is usually very limited. Often, cloud service providers offer a public product of extensive user action which has an overall SLA and standards to all customers of which there is no room to negotiate additional security checks which should implement service provider.[15] Often, cloud service providers lack of transparency in their operations. This makes cloud service providers to not have sufficient credibility for hosting security of information systems that have an impact medium or high security of data even for those who have low impact. On the other hand, users try to exploit every opportunity to push transparency security of cloud service providers. It is common for service providers trying to contract respectively agreement where the provisions dealing with transparency, especially those dealing with audit to overlook, as it cut the cost of expenses, but it does not contribute to reliability security offering for their services. [13]

2.4. Lack of adequate standards

International organizations and institutions dealing with standardization and certification of information technology platforms, yet have failed to issue a specific standard that has to do with cloud computing. Right now, standardization and certification of services of this technology is based on several standards that apply to the overall assessment of quality and safety in information technology such as ISO 27001, SAS70, etc. (FISMA)

3. Proposal

3.1. Definition of key points for reliability

Data storage in cloud computing as it told earlier in this paper, comprises three main aspects related with the security in information technology, which are: confidentiality, integrity and availability. The combination of these three objectives and research about them in a single theme is heavy work for the period provided for this research. Also, restrictions on the number of words for the topics explored, prevent the expansion of the detailed research. Thus, this research is focused on one of the objectives of safety of enterprises data storage in cloud computing taking on three case studies from multiple bidders already in cloud services.
According to the case, confidence in cloud services based on key points which are determined by the service level agreement (*Service Level Agreement).* In accordance with the Alliance for Security in the Cloud, we can define key points at which individuals and enterprises use cloud computing should base storage reliability of their data, which are:

1) Identification and Access Management, provides the only access to authorized users.
2) Data Loss Prevention, ensures that the data can not be deleted without authorization.
3) Web Security, protects customers from downloading content that endanger IT system.
4) Email Security, protects clients from receiving and sending emails that threaten IT system.
5) Security Assessments, requires implementation of standards such as ISO, SAS etc.

6) Intrusion Management, enables timely detection and prevention interventions that threaten the IT system.
7) Security Information and Event Management, enables customers to familiarize themselves with security flaws.
8) Encryption, provides data protection from eavesdropping and unauthorized access.
9) Business Continuity and Disaster Recovery, this option allows customers or service way back after a problem.
10) Computer Network Security, provides mechanisms to prevent unauthorized physical access or remotely on IT resources.

These key points of reliability can be provided or not by the provider of cloud computing services. Below will be presented how the cloud service providers offer and allow the application of these security issues. As the case study are taken three well-known companies in the field of cloud services that are Amazon, Google and Microsoft.

3.2. Comparing the performance of the key points of the reliability of Amazon, Google and Microsoft

Research has result as it is shown in comparison table between the three case studies in the fulfillment of the ten key points of reliability for data storage in cloud computing.[16] [17] [18]

Table 1. Comparative table of the key points of reliability. With letter "X" are shown the fulfilled points of reliability by cloud service providers which are used as case studies.

No.	Key points of the reliability in security	Case studies		
		Amazon	**Google**	**Microsoft**
1)	**Identification and Access Management**	X	X	X
2)	**Data Loss Prevention**	X	X	X
3)	**Web Security**		X	
4)	**Security for Email**	X	X	X
5)	**Security Assessment**	X	X	X
6)	**Intrusion Management**			
7)	**Security Information and Event Management**	X		X
8)	**Encryption**	X		X
9)	**Business Continuity and Disaster Recovery**	X	X	X
10)	**Computer Network Security**	X	X	X

Conclusion

In conclusion, the results of research conducted shows that cloud service providers already offer diversity in terms of reliability for data storage to customers and enterprises that identify the quality of service they provide. This makes users when making the selection of service providers, consider the type of service you require to tune the security offered. Architectures described in the introduction of this work also affect the reliability of data storage and selection of models that users should be considered for storage of their data, which depends on the conditions offered by its service provider.

Outcomes of reliability as key points clearly demonstrate the safety requirements which should address individuals and enterprises especially when dealing with the reliability of data storage in the cloud. Meeting these key security points by cloud services providers proves the quality of the

service provided in terms of reliability. Also, research found out that there is still no standardized certification for security assessment, meeting the requirements of which will facilitate the achievement of reliability in storing data in the cloud. ISO 27001 is the only standard for security evaluation that although no mention of cloud services and does not include sufficient aspects of reliability of cloud services, the case studies in this research shows that it is supported from Amazon and Microsoft, but not by Google.

Evaluation of the qualitative characteristics of cloud computing as well as the fulfillment of the key points of reliability that were mentioned above, makes the selection of cloud service providers in terms of reliability in storing data to be straight and unmistakable. This facilitates customer ambiguities that may have for cloud computing services offered through it or the selection of providers of these services. It is expected that by 2016, the organization which deals with the issuance of ISO publish a special certification standard for cloud computing services that will be recognized as ISO 27017. Until then, customers and enterprises remains that for the storage of their data in the cloud, reliability on service providers can be based on the information distributed from this research results, which is worked with great dedication and, which certainly can be completed and processed even more.

References

1. NIST Posted by.*SP800-145: The NIST Definition of Cloud Computing.* [Online].Available from:http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.[Accessed, 11.01.2016].
2. CloudTweaks, Posted by. *Demystifying SaaS, PaaS and IaaS* [online] Available from: http://www.cloudtweaks.com/2010/05/cloud-computing-demystifying-saas-paas-and-iaas [Accessed, 21.12.2015].
3. Webopedia, Posted by.*SaaS - Software as a Service, Storage as a Service* [online] Available from: http://www.webopedia.com/TERM/S/SaaS.html [Accessed, 21.12.2015].
4. Malcolm D. Posted by.*The Five Defining Characteristics of cloud computing* [online] Available from: http://www.zdnet.com/news/the-five-defining-characteristics-of-cloud-computing/287001 [Accessed, 12/21/15].
5. Reiter S. Posted by.Project ascensia Blo, *Dreaming of fluffy clouds.* [Online] Available from:http://blog.ascens-ist.eu/2011/03/dreaming-of-fluffy-clouds/ [Accessed, 24.12.2015].
6. Curino, C. Jones, V., Zhang, Y., Wu, E. and Madden, S.Posted by. *The Case for a Database Service* [online] Available from: http://www.mit.edu/~eugenewu/files/papers/caseforrelationalcloud.pdf [Accessed, 21.12.2015].
7. Rouse, M. Posted by.*Network-as-a-Service (NAAS)* [online] Available from: http://searchsdn.techtarget.com/definition/Network-as-a-Service-NaaS [Accessed, 21.12.2015].
8. Hendryx, A., Posted by.*Cloudy Concepts: IaaS, PaaS, SaaS, Maas,* CAAS & XaaS [online] Available from: http://www.zdnet.com/cloudy-concepts-iaas-paas-saas-maas- caas-and-xaas-4010024679 [Accessed, 12/21/15].
9. Antonopoulos, N. and L. Gillam(2010). *Cloud Computing.*London: Springer-Verlag Limited.

10. Landis, C. and Blacharski, D.(2010). *Cloud Computing Made Easy*.Morgantown Virtual Global, Inc.
11. NIST. (2008c).SP 800-53. Posted by.(2009) *Guide for Assessing the Security Controls in Federal Information Systems.* [Online] Available from: http://csrc.nist.gov/publications/PubsSPs.html [Accessed, 24.12.2015].
12. NIST. (2009b), SP 800-53, (12 August 2009).*Recommended Security Controls for Federal Information Systems and Organizations.* [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated- errata_05-01-2010.pdf [Accessed, 24.12.2015].
13. Amazon.Posted by. *AWS Security and Compliance Center*. [Online] Available from: http://aws.amazon.com/security/ [Accessed, 24.12.2015].
14. Google.Posted by. Google's Approach to IT Security. [Online] Available from: https://cloud.google.com/files/Google-CommonSecurity-WhitePaper-v1.4.pdf [Accessed, 24.12.2015]
15. Kaufman, C. and Venkatapathy, R.(2010). Windows Azure Security Overview. [Online] Available from: http://go.microsoft.com/?linkid = 9740388 [Accessed, 24.12.2015]