Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 133 (2019) 53560-53563

ISSN: 2229-712X

What are the Security Risks Associated with the use of Cloud Computing?

Hamad Saif Al-Neyadi

College of Engineering, Abu Dhabi University Alain Road, Abu Dhabi, United Arab Emirates.

ARTICLE INFO

Article history:

Received: 20 July 2019;

Received in revised form:

20 August 2019;

Accepted: 31 August 2019;

Keywords

Cloud Computing,

Security.

ABSTRACT

Organizations came to the realization that it is not economically feasible to maintain the increasing maintenance costs of maintaining data centers with large floor space. One of the main concerns associated with Cloud Computing is the security of the service is that sensitive and important data is no longer only under the control of the data owner as the service provider also has access to that data. In terms of the methodological approach used by this thesis, this thesis will utilize the use of the qualitative method in answering the research questions posed by this thesis. The systematic literature review has shown that there are novel and innovative ways for organizations to mitigate the inherent risks associated with the use of cloud computing.

Introduction

Cloud Computing (CC hereafter) is an attractive tool for organizations to reduce costs associated with IT infrastructure such as IT infrastructure, personnel costs, computer access and storage by outsourcing it to a third party which provides these services to these organization off site and cyber space (Bendandi, 2009). While CC is clearly an attractive source for organizations in terms of cost benefit analysis like for example the reduce costs of cloud subscription, another advantage for using CC is that the organization will rely on the security measures of the CC service provider that clearly surpasses the capabilities of most of the organizations that use CC (Singel, 2009). Alternatively, since CC is provided by a Third Party Service Provider (TPSP); there are also serious and important drawbacks of using CC and the most glaring default of CC from an organizational perspective is the safety of the information or data kept by TPSP (Schillace, 2010).

Aim and objectives

The main aim of this thesis is to examine the security risks attached to the use of Cloud Computing and to examine whether such risks outweigh the benefits of the use of this technology. In terms of this thesis's objectives; they are: a) Examine the infrastructure that Cloud Computing Service Providers use for both their commercial and private consumers. b) Examine the security risks and threats attached to the use of cloud computing c) Assess and analyze the cost to benefit analysis in the use of cloud computing by private and commercial consumers.

II. Literature review

a) What is Cloud Computing? In the early 1990sand before the mass use of the Internet, the IT community came to the realization that it is not economically feasible to maintain the increasing maintenance costs of maintaining data centers with large floor space that requires large amount of power for operation and cooling of equipment and infrastructure (Cohen, Farber, Fontecilla, 2008). As a result, this led the IT community to develop and to adopt grid computing (networks or in other words a series of computers linked to one mainframe) and then virtualization (which allows more than one user on a single computer) (Edwards, 2009). Cloud computing was the next in the evolution process which in essence provides both grid computing benefits and virtualization benefits remotely. What is meant by remotely is that the end user only has to access the site of the cloud computing service provider and this access can be made remotely or in other words from anywhere as long as the end user has access to the internet thus the end user does not need to be using a computer on a grid (on site network computer) as well as having the ability of others to access the same service provider (virtualization) again without having to be physically present on site (Lillard and Garrison, 2010). The difference between Cloud Computing and mainframes and servers is that the formers required huge initial investment by the organization to set up the IT infrastructure while in Cloud Computing the organization pays for the use of the Cloud as a service or as a pay as you go utility bill. The advantages of paying for IT infrastructure and use as a utility as opposed to setting up a IT infrastructure is clearly the cost associated with both (Lillard and Garrison, 2010). . This is because unlike mainframes and servers; Cloud Computing service providers have the ability to provide the end user with a shared pool of IT configurable resources such as information and storage facilities; processing and network facilities as well as software access. b) Architecture of Cloud Computing In terms of its architecture; Cloud Computing differs from traditional IT infrastructure in that it allows remote access to end user. The building blocks of Cloud Computing is more complex than remote access, this is because Cloud Computing comprises of both hardware and software architecture that enables Cloud Computing to provide a service for the fraction of the cost of onsite IT infrastructure that in turns enables Cloud Computing to upscale through virtualization (Erdogmus, 2009; Edwards, 2010). Therefore, the simplest way to describe the Cloud Computing architecture comprises of 'cloud services' (measured service) supplied by 'cloud service providers' (third parties; suppliers or brokers) to 'cloud consumers' (end users both commercial and private entities) over a networked online or private

Tele:

E-mail address: 1066122@students.adu.ac.ae

infrastructure (Lillard and Garrison, 2010). Furthermore, Cloud Computing infrastructure is based on 4 core layers namely a) hardware; b) software; c) virtualization and d) applications. With regards to hardware what is meant here are the physical components of Cloud Computing namely servers and network components. With regards to software what is meant here is the operating system that is required to run the Cloud Computing apparatus. With regards to virtualization what is meant here is that Cloud Computing enables pooling of resources as well as sharing of computer resources. With regards to applications what is meant here is the added value services provided by Cloud Computing service providers like Google and Amazon products associated with use of their Cloud Computing service (Smith, 2008; Tribhuwan, Bhuyar and Pirzade, 2011). Finally, it is important to highlight that Cloud Computing is like any hosted type service delivered online through an online network. Saying that though, Cloud Computing is broadly divided into three categories namely Infrastructure as a Service (IaaS) which includes the entire Cloud Computing Infrastructure. The second is Platform as a Service (PaaS) which sits on top of the IaaS and it aims to provide programming languages and tools as well as application development capabilities and finally there is Software as a Service (SaaS) which rests on both IaaS and PaaS and provides services such as presentation, application and management capabilities (Heiser and Nicolett, 2008). It is worth noting that it is the SaaS that is licensed and traded to most consumers of Cloud Computing services. This is because the SaaS in most instances provide the use and functionality of Cloud Computing to private consumers and most small and medium sized businesses who are only interested in the storage aspect of Cloud Computing and not the infrastructure or Platform types of Cloud Computing. c) Benefits of Cloud Computing In terms of the benefits of Cloud Computing; these are endless and non exhaustive. The beginning point is that Cloud Computing provides excellent savings in costs particularly for an organization in terms of lower start up costs and maintenance. In addition, the introduction of Cloud Computing in the workplace removed ancillary costs such as cost of energy and cooling (onsite infrastructure required 24 access to electricity); floor space; reduction in operational costs and most importantly Cloud Computing provides a pay as you go measured service which means that organization only pays when the Cloud Computing to use (Mather, Kumaraswamy, and Latif, 2009). Alternatively, Cloud Computing also allows organizations to be more competitive by diverting funds from the expensive onsite IT infrastructure to their business and it also allows the organizations to be flexible and agile platforms for computing by providing scalability and the instant use of high performance resources that are very reliable (Benslimane, Plaisent, Bernard, Bahli, 2014). In addition, Cloud Computing allows organizations IT departments now save money on application use and development; deployment; security and maintenance time and costs while also benefitting from the fact that using Cloud Computing allows organizations to be green in their power use and green in their economies of scale which Cloud Computing allows (West, 2010a). d) Risks associated with Cloud Computing Cloud Computing like any other technology comes with serious drawbacks and one of the main concerns associated with Cloud Computing is the security of the service. This is because the business model of Cloud Computing requires individuals and organizations to host their data with the service provider which in most times are an independent third party service provider like for example Amazon cloud services (Maghrabi, Pfluegel, Noorji, 2016). This means that sensitive and important data is no longer only under the control of the data owner as the service provider also has access to that data. This means that if the service provider's security is breached; that data could be compromised, stolen or destroyed hence the vulnerabilities of Cloud Computing comes from the threat of breach of Cloud Computing service provider's infrastructure that contains the data of its service end users (West, 2010b).

Also because Cloud Computing relies on remote access; pooling resources and scalability (which it is unique selling point), it is this that makes Cloud Computing vulnerable. As these services allows Cloud Computing to host applications and to share infrastructure which in turn increases exponentially raises the risk of potential unauthorized access and raises other major concerns like concerns over privacy of the data (Whitten, 2010). Alternatively, Cloud Computing has other concerns such as issues with identity management as well as issues such as compliance; authentication; integrity and confidentiality; encryption level; availability of data and the network and physical security of the Cloud Computing infrastructure. In addition; there are also inherent problems associated with Cloud Computing other than infrastructure problems such as legal problems like for example the contractual agreements between the service provider and the end user; quality of Cloud Computing Services; data application management; vendor lock in; performance of the Cloud Computing service and its availability to the end user when they want to use it (Zetter, 2010). e) Development Operations (DevOps) This proposal will not be complete without mentioning an important aspect that is integral to Cloud Computing technology which is Development Operations also known as DevOps.

In its basic definition, DevOps is the automation process that allows developers to interact with their software in real time and without the need of waiting or latency (Ju, Soares, Shin, Ryu and Silva, 2013). In other words, DevOps simplifies, and speeds up the ability of the content provider i.e. the developer to interact with the organizations using the content i.e. businesses using the software and to respond in real time to the needs of this business, it is here that the Cloud Computing technology comes in as it all0ows DevOps to use the centralized aspect of Cloud Computing to provide real time services to consumers of their products (Murphy, Gallant, Gaughan and Diego, 2012).

This relationship between DevOps and Cloud Computing is symbiotic in nature because: i) DEvOps that are cloud based are less likely to require resource leverage thus making them easier to operate at a large scale. By that cloud DevOPs will use the cloud system to track applications, developers; users etc (Miglierina, 2014; Dyck, Penners and Lichter, 2015) ii) DEvOps that are cloud based are more likely to in testing, deployment and production of software unlike its non cloud counterpart. This is because cloud Devops use the cloud platform to conduct all these activities while non cloud Devops have to use a number of platforms (raising cost and time) in order to perform the same functions (Bayser, Azevedo and Cerqueira, 2015; Gottesheim, 2015).

III. Methodology

In terms of the methodological approach used by this thesis, this thesis will utilize the use of the qualitative method in answering the research questions posed by this thesis. This

is because by utilizing this method, the researcher will be able to use secondary sources to answer the central problem statement of this thesis namely examine the phenomenon that is Cloud Computing from a security perspective in terms of the measures or the lack of measures undertaken by Cloud Computing Service Providers in protecting the important and private data of their private and commercial consumers (Bryman, 2012).

In terms of the data collection method of this researcher; the researcher aims to utilize in the range of (ñ-35) and (n-40) secondary sources which will include and not limited to academic books; peer reviewed journals and articles as well as industry specific newspaper articles. These secondary sources will be sourced from a variety of databases including Elite and ProQuest Central (Crow and Semmens, 2008).

IV. Results

In terms of the results of the systematic literature review the security risks associated with the use of cloud computing range from the breach of data; privacy issues such as unauthorized access to data and potential legal ramification like a breach of public data. In terms of security techniques to mitigate security risks associated with cloud computing, they are as follows: Benslimane et al (2014) conducted a review of the most up to date security techniques used by cloud computing services in order to provide an effective and secure cloud computing services. This review also ranks 12 cloud computing providers based on their security like for example the providers level of encryption; providers ability to segregate data for enhanced security as well as the transparency of the cloud computing provider to how data is stored and used. Edwards (2009), offers encryption as a viable technique to overcome cloud computing dispersed nature that inherently makes it difficult for users of this technology to ensure that logging procedures are adhered or to track unauthorized use or activity. He goes further and offer encryption even when cloud computing is used in a safe and secure environment because it mitigates the risk of data breach in a shared environment especially where a party has authorization to use the cloud but do not have authorization to view certain data due to its high classification like for example state secrets or commercial sectors Maghrabi et al (2016) advocates the use of a novel idea adopted from the game theory namely the OCTAVE method of risk assessment. Here the authors argue that to mitigate the use of cloud computing; an organization must first identify what is at risk before then identifying the assets whether real, cyber or people that the organization feels is the invaluable to the business before finding threats to these identified assets. Once the asset and threat are both identified, then the organization identifies the risk associated and mitigate accordingly. Finally, the authors a score based system to rank threats from serious and immediate to low risk that aims to help cloud computing users to weigh up the risk involved with this technology Heiser and Nicolett (2008) this book provides a comprehensive analysis of possible security risk documented against a cloud computing provider. For example the book sets a test on how to assess risk when dealing in cloud computing as well as providing a non exhaustive list of compliance requirements and good practice rules that cloud computing providers must apply to minimize and mitigate risk to their users. In summary, the systematic literature review has shown that there are novel and innovative ways for organizations to mitigate the inherent risks associated with the use of cloud computing. From basic solution like encryption to a more complicated and labor intensive task like OCTAVE for example suggest that over time, cloud computing users will develop a more secure environment for the use and transference of data with minimized an mitigated level of risk.

V. Conclusion

In summary, this thesis will aim to explore a less talked about aspect of Cloud Computing and that is the security protection or lack of protection afforded to the end users of this technology. This will be done through a close forensic examination of the evidence for and against the use of Cloud Computing in regards to its security measures. This thesis will then evaluate all the data collected and make a determination on the balance of the evidence whether the security lapses and security breaches deter future users from using this technology despite all the obvious benefits of using this technology.

References

[1] Dyck, R. Penners, and H. Lichter. (2015). Towards definitions for release engineering and devops. In 3rd IEEE/ACM International Workshop on Release Engineering, RELENG 2015, Florence, Italy, May 19, 2015, page 3.

[2] Bendandi, S. (2009). Cloud computing: Benefits, risks and recommendations for information security.Retrieved on April27,2019fromhttp://www.scribd.com/doc/23185511/Cloud-Computingbenefits-risks-and-recommendationsfor-information-security.

[3] Bryman, A. (2012).Social research methods. Oxford: Oxford University Press.

[4] Cohen, D. Farber, M. Fontecilla, R. (2008).Cloud computing a transition methodology. Booz Allen Hamilton. Retrieved on April 27, 2019 from http://www.boozallen.com/ media/file/cloudcomputingtransition-methodology.pdf.

[5] Crow, I., Semmens, N. (2008).Researching criminology. Maidenhead: Open University Press.

[6] Edwards, J. (2009).Cutting through the fog of cloud security. Computerworld. Framingham: Feb 23, 2009. Vol. 43, Iss. 8; pg. 26, 3 pgs.

[7] Edwards, J. (2010).Defending the cloud - and your business. Webhostingunleashed.com. Retrieved on April 27, 2019 from http://www.webhostingunleashed.com/features /defendingcloud090208/.

[8] Greene, T. (2009). New attacks on cloud services call for due diligence. Network World. Southborough: Sep 14, 2009. Vol. 26, Iss. 28; pg. 8, 1 pgs. Retrieved on April 27, 2019 fromhttp://www.networkworld.com/newsletters/vpn/2009/090709cloudsec2.html.

[9] H. Erdogmus, (2009)"Cloud computing: Does nirvana hide behind the nebula?," Software, IEEE, vol. 26, pp. 4-6.

[10] J. Heiser and M. Nicolett, (2008)."Assessing the security risks of cloud computing," Gartner Report.

[11] Louai Maghrabi, Eckhard Pfluegel, Senna Fathima Noorji, (2016). "Designing utility functions for game-theoretic cloud security assessment: a case for using the common vulnerability scoring system", Cyber Security And Protection,Of Digital Services (Cyber Security) 2016 International Conference On, pp. 1-6,

[12] M. de Bayser, L. G. Azevedo, and R. F. G. Cerqueira. (2015). Research ops: The case for devops in scientific applications. In IFIP/IEEE International Symposium on Integrated Network Management, IM 2015, Ottawa, ON, Canada, 11-15 May, 2015, pages 1398-1404.

[13] M. Miglierina. (2014). Application deployment and management in the cloud. In 16th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2014, Timisoara, Romania, September 22-25, 2014, pages 422-428.

[14] M. Tribhuwan, V. Bhuyar, and S. Pirzade,(2010). ”Ensuring Data Storage Security in Cloud Computing through Two-Way Handshake Based on Token Management,” in Advances in Recent Technologies in Communication and Computing (ARTCom), 2010 International Conference, pp. 386-389.

[15] S. Murphy, S. Gallant, C. Gaughan, and M. Diego. (2012). U.S. army modeling and simulation executable architecture deployment cloud virtualization strategy. In 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, CCGrid 2012, Ottawa, Canada, May 13-16, pages 880-885.

[16] Sinclair, S. and Smith, S.W., (2008). “Preventative directions for insider threat mitigation via access control”. In Insider Attack and Cyber Security (pp. 165-194). Springer, Boston, MA.

[17] Stolfo, S.J., Bellovin, S.M., Hershkop, S., Keromytis, A.D., Sinclair, S. and Smith, S.W. eds., (2008). “Insider attack and cyber security: beyond the hacker” (Vol. 39). Springer Science Business Media.

[18] Schillace, Sam. (2012). “Default https acces for Gmail.” Gmail Blog. January 12, 2010 Retrieved on April 27, 2019 from http://gmailblog.blogspot.com/2010/01/default-https-access-forgmail.html.

[19] Singel, Ryan. (2009).”Encrypt the Cloud, Security Luminaries Tell Google.” Wired Threat Level, Retrieved on April 27, 2019 from http://www.wired.com/ threatlevel/2009/ 06/googlessl/.