Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 7, Issue, 03, pp.13537-13540, March, 2015

INTERNATIONAL JOURNAL
OF CURRENT RESEARCH

ISSN: 0975-833X

REVIEW ARTICLE

A STUDY ON THE DISRUPTIVE VIS-A-VIS CHAOTIC NATURE OF CLOUD COMPUTING DEPLOYMENT AND SERVICE DELIVERY MODELS

*Prof. Gayathri Ranjit

Assistant Professor - Operations, TKM Institute of Management, Karuvelil, Kollam

ARTICLE INFO

Article History:
Received 09th December, 2014
Received in revised form
24th January, 2015
Accepted 16th February, 2015
Published online 17th March, 2015

Key words:

Cloud security, data security, cloud computing, disruptive technology

ABSTRACT

Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Three criteria are assessed in characterizing cloud computing as a disruptive technology (Christensen, 2002). First, cloud computing as an innovation, must enable less-skilled and/or less-wealthy individuals to receive the same utility as only the more-skilled and/or more-wealthy intermediaries could formerly attain. Second, cloud computing must target customers at the low end of a market with modest demands on performance, but with a performance trajectory capable of exceeding those demands and thus taking over markets, tier by tier. Third, an ecosystem in the form of a fully integrated single entity or a set of modular entities is required to successfully support the disruptive innovation. However, current cloud computing solutions lack sufficient security and customer control. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. This paper analyses cloud computing as a disruptive and chaotic technology and also analyses the various deployment and service delivery models.

INTRODUCTION

Cloud computing is a next generation computing platform that helps the users to share the resources through communication mediums. According to National Institute of Standards and Technology (NIST) one of the most accepted definition of cloud computing is “Cloud computing is a model for enabling ubiquitous, 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”. European Community for Software and Software Services (ECSS) defines “cloud computing as the delivery of computational resources from a location other than your current one”. So in simple words cloud computing can be defined as a distributed computing environment that enables the users to access and exchange their resources (applications and data) remotely and provides services to use the remote hardware and software within a network without the knowledge of technological infrastructure. Companies, large and small, are moving quickly to adopt some form of cloud computing tools and services, recognizing a new technology that could reshape their competitive landscape.

In a new global survey of nearly 1,500 business and technology leaders conducted by Harvard Business Review Analytic Services, the majority — 85% — said their organizations will be using cloud tools moderately to extensively over the next three years. They cited the cloud’s ability to increase business speed and agility, lower costs, and enable new means of growth, innovation, and collaboration as the drivers for this fairly aggressive rate of adoption.

Literature Review

Gartner 2008 identified seven security issues that need to be addressed before enterprises consider switching to the cloud computing model. They are as follows: (1) privileged user access - information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water, (2) regulatory compliance - clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by 3rd party organizations that check levels of security and providers that don't (3) data location – depending on contracts, some clients might never know what country or what jurisdiction their data is located (4) data segregation - encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider. (5) recovery - every provider should have a disaster recovery protocol to protect user data (6) investigative support - if a client suspects faulty activity from the provider, it may not have many legal ways pursue an investigation (7) long-term viability - refers to the ability to retract a contract and all data if the current provider is bought out by another firm. The Cloud Computing Use Case Discussion Group discusses the different Use Case

Corresponding author: Gayathri Ranjit
Department of Business Administration, College of Engineering, Trivandrum

scenarios and related requirements that may exist in the cloud model. They consider use cases from different perspectives including customers, developers and security engineers. ENISA investigated the different security risks related to adopting cloud computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in the cloud computing may lead to such risks.[4] Balachandra *et al*. 2009 discussed the security SLA's specification and objectives related to data locations, segregation and data recovery. Kresimir *et al*, 2010 discussed high level security concerns in the cloud computing model such as data integrity, payment and privacy of sensitive information.

Bernd *et al.* 2010 discuss the security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology-related, cloud characteristics-related, security controls related. Subashini *et al*. discuss the security challenges of the cloud service delivery model,focusing on the SaaS model [8]. Ragovind *et al*. (2010) discussed the management of security in Cloud computing focusing on Gartner's list on cloud security issues and the findings from the International Data Corporation enterprise. Morsy *et al*. 2010 investigated cloud computing problems from the cloud architecture, cloud offered characteristics, cloud stakeholders, and cloud service delivery models perspectives. A recent survey by Cloud Security Alliance (CSA) & IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing growth. Several studies have been carried out relating to security issues in cloud computing but this work presents a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing deployment types and the service delivery types.

Cloud Deployment and Service Delivery Models and Issues

Cloud Deployment Models

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand as depicted in Figure 2. The Cloud Computing model has three main deployment models which are:

Private cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.

Public cloud

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. [13] Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

Hybrid cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [14]. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets -for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.

Cloud Computing Service Delivery Models

Following on the cloud deployment models, the next security consideration relates to the various cloud computing service delivery models. The three main cloud service delivery models are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

Infrastructure as a Service (IaaS)

Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware such as servers, networking devices and processing power. They also allow varying degrees of financial and functional flexibility not found in internal data centers or with collocation services, because computing resources can be added or released much more quickly and cost-effectively than in an internal data center or with a collocation service [2]. IaaS and other associated services have enabled startups and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS completely abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities.

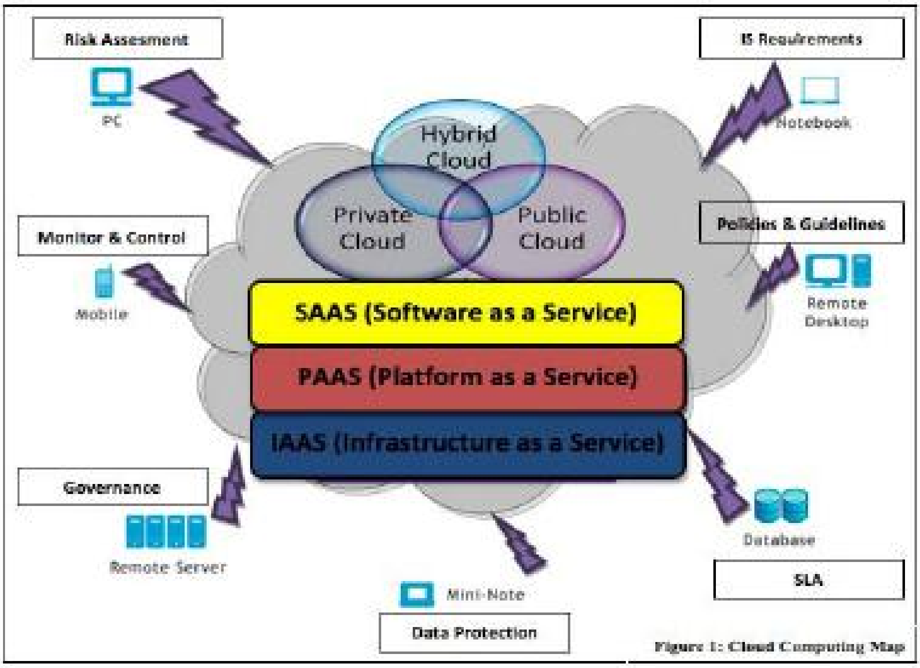
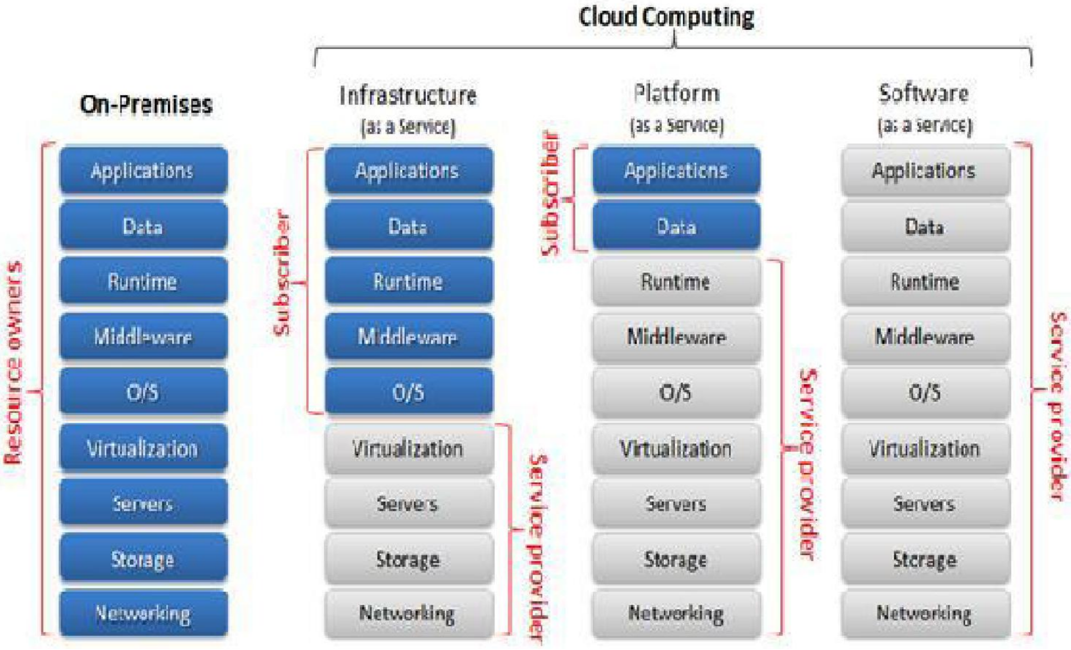


FIGURE 2: Cloud deployment model [13]



The cloud has a compelling value proposition in terms of cost, but 'out of the box' IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security provided at the host.

Platform as a service (PaaS)

Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the provider's servers. It is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development life cycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the "view" of the developers. Platform as a service cloud layer works like IaaS but it provides an additional level of 'rented' functionality.

Clients using PaaS services transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some degree of lock-in posed by the additional functionality layers

[14]. The use of virtual machines act as a catalyst in the PaaS layer in Cloud computing. Virtual machines must be protected against malicious attacks such as cloud malware. Therefore maintaining the integrity of applications and well enforcing accurate authentication checks during the transfer of data across the entire networking channels is fundamental.

Software as a Service

Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches become popular. SaaS is also often associated with a pay-as-you-go subscription licensing model. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. SaaS is most often implemented to provide business software functionality to enterprise customers at a low cost while allowing those customers to obtain the same benefits of commercially licensed, internally operated software without the associated complexity of installation, management, support, licensing, and high initial cost.

The architecture of SaaS-based applications is specifically designed to support many concurrent users (multitenancy) at once. Software as a service applications are accessed using web browsers over the Internet therefore web browser security is vitally important. Information security officers will need to consider various methods of securing SaaS applications. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the Internet.[8]

Conclusion

There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. Despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding the momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. Despite the trumpeted business and technical advantages of cloud computing, many potential cloud users have yet to join the cloud, and those major corporations that are cloud users are for the most part putting only their less sensitive data in the cloud. Lack of control is transparency in the cloud implementation – somewhat contrary to the original promise of cloud computing in which cloud implementation is not relevant. Transparency is needed for regulatory reasons and to ease concern over the potential for data breaches. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

REFERENCES

International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011 254 Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010.

Balachandra, R. K. , Ramakrishna, P. V. and Rakshit, A. 2009. “Cloud Security Issues.” In PROC ‘09 IEEE International Conference on Services Computing, pp 517-520.

Kresimir, P. and Zeljko, H. 2010. "Cloud computing security issues and challenges.." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, pp. 344-349.

Grobauer, B., Walloschek, T. and Stöcker, E. 2010. "Understanding Cloud Computing Vulnerabilities," *IEEE Security and Privacy*, vol. 99,

Subashini, S. and Kavitha, V. 2010. “A survey on security issues in service delivery models of cloud computing.” *J Network Comput Appl* doi:10.1016/j.jnca.2010.07.006. Jul., 2010.

Ramgovind, S., Eloff, M. M. and Smith, E. 2010. “The Management of Security in Cloud Computing” In PROC 2010 IEEE International Conference on Cloud Computing.

Morsy, M. A. , Grundy, J. and Müller, I. 2010. “An Analysis of the Cloud Computing Security Problem” In PROC APSEC 2010 Cloud Workshop.

A Platform Computing Whitepaper. “Enterprise Cloud Computing: Transforming IT.” *Platform Computing*, pp6, 2010.

Brodkin, J. Jun, 2008. “Gartner: Seven cloud-computing security risks.” *Infoworld*, Available: <http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity- risks-853?page=0,1> Mar. 13, 2009.

Gens, F. Feb, 2009 . “New IDC IT Cloud Services Survey: Top Benefits and Challenges”, *IDC eXchange*, Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].

ENISA. Feb, 2009. "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment [Jul. 10, 2010].

Arnold, S. 2009, Jul. “Cloud computing and the issue of privacy.” *KM World*, pp14-22. Available: www.kmworld.com Aug. 19, 2009.

Cloud Security Alliance (CSA). Mar.19,2010. Available: http://www.cloudsecurityalliance.org

****