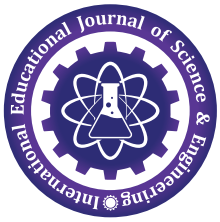
Computer Science

E-ISSN No : 2581-6195 | Volume : 2 | Issue : 1 | Jan-Feb 2019



CLOUD COMPUTING MODELS: A STRATEGY FOR THE DEVELOPMENT OF NEW MARKETS FOR CLOUD SERVICES AND DEVELOPMENT MODELS

Amanze, B.C.[1], Chilaka. U.L[2]

ABSTRACT

This work will look into the available cloud models being offered in the market and classify the various forms of cloud. We shall also look at the security of the cloud, its challenges and probable solutions to these challenges. The capabilities of the cloud providers would be used to expatiate on what these service providers do and what they do not offer. It should be known that cloud computing utilizes various technologies that have been in existence since ages. This has led to the renewal of building an IT infrastructure from various approaches. Also we shall prove that cloud computing relies on sharing of various IT infrastructures like: network (internet), server's storage, applications, services and what have you.

KEYWORDS: Cloud Computing, Models, Cloud Services, Delivery Models

INTRODUCTION

What we call cloud computing these days date back to the 60s with the emergence of time sharing systems of mainframe systems. But because of huge cost of hardware infrastructure and users being unable to control the performance of the hardware costs and this personal computers gave users a greater control of their hardware/software resources.

With the emergence of personal computing, a new challenge of data sharing became obvious. The client service architecture become more complex, these problems skyrocketed into huge costs in management and IT infrastructure. Consequently, costs of software development in many organizations was reduced compared to software and infrastructure maintenance, Florin (2012).

Usefulness of Cloud Computing

Most organizations that start business newly cannot invest in infrastructures like software or hardware that would be cost effective, rather they would prefer to subscribe for such services as pay as you grow. The quest for e-commerce, social media and other web services has tremendously increased the demand for computational resources. Consequent upon this, companies like Google, Amazon and Microsoft quickly realized that financially it is more feasible to build very large data centers for their needs. The goes to show that it will be much cost efficient to buy resources like electricity bandwidth, and storage in large volumes. Because of expertise and specialization in certain areas, companies like Amazon, Google built large public cloud data centers and offer computing services to other companies. It should be known that the downward trend in the cost of hardware and architecture standardization and mechanical compatibility resulted in low cost of computational costs, Reese (2009).

Hardware virtualization has allowed the increasing hardware utilization density and ensure that hardware resources are utilized efficiently. Open source software and commodity hardware have enhanced the development of cloud computing of which Linux Operating System stands as a building block. At the same time, virtualization software like Xen is used by Amazon to host the largest set of virtual machines. The ability to avoid expensive software license costs in one of the factors that enables companies to provide affordable cloud services.

Cloud computing is a subscription based service where you can obtain networked storage space and computer resources. To expatiate on this think of your e-mail, which could be housed by either yahoo, or g-mail or hotmail and so on. These companies house all of the hardware and software necessary to support your personal e-mail account, Dukaric et al. (2013).

Note that your email is not housed on your physical computer, you access it through an internet connection and you can access it anywhere. If you are on a trip, at work, or down the street, you can check up your e-mail account, as long as you have access to the internet. Your e-mail software is different from the software installed on your computer such as your word processing software. The cloud makes it possible

[1,2]Department of Computer Science, Imo State University, Owerri

HOW TO CITE THIS ARTICLE:
Amanze, B.C., & Chilaka. U.L. (2019). Cloud Computing Models: A Strategy for The Development of New Markets for Cloud Services and Development Models, International Educational Journal of Science and Engineering (IEJSE), Vol: 2, Issue: 1, 08-11

Research Paper

for you to access your information from anywhere at any time. Originally, computer setup requires you be in the same location as your data storage device, but the cloud takes away that. The cloud removes the need for you to be in the same physical location as the hardware that stores your data. Your cloud provider can both own and house the hardware and software necessary to run your home.

Types of Cloud

We have different types of clouds. They are the public cloud which can be accessed by any subscriber with internet connection and access to the cloud space. There are also private clouds which can be only available to the private owner. The community cloud is the one shared by two or more organizations that have similar cloud requirements. A hybrid cloud involves combination of at least two clouds which could be a Private, Public or Community clouds.

Compatibilities of the cloud service provider

The cloud provider you decided to subscribe to must fulfill your specific cloud needs. Also at each instance a provider must at least allow you reasonable control over their cloud. Your needs would vary depending on how you wish to utilize the cloud space allotted to you. We have three types of providers: software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS). One important fact is that the amount of control you have over your information varies as well as what you expect your cloud provider to do for you.

1. SAAS: Here, the provider allows subscribers access to both software resources and applications. You will have the same software on all your devices at once just by accessing it on the cloud.
2. PAAS: Here, the provider gives subscribers access to the components that they need to develop and operate application over the internet.
3. IAAS: This type deals with computational infrastructure. The subscriber completely outsources the storage and resources, such as hardware and software that they need.

The overall rule we can conclude here is that the subscriber gains more control of the cloud and its resources from SaaS down to IaaS. It should be noted that the free and low cost cloud services such as the web –based e-mail is the commonest of the clouds you can subscribe to, and is not concerned with other complex cloud offerings.

Security of the Cloud

The value you attach to the information you store in your cloud, makes it critical for you to understand the security measures that your cloud provider has in place or should put in place to secure your data in the cloud. The type of encryption method your provider uses as well as their method of hardware are both critical to the security of data in the cloud. You should ask questions like: Do they have backups, do they have firewall setup, and in a community cloud what barriers are there to forestall to keep your information or data separate from other companies or other peoples information.

Security for cloud computing environment is non-compromising requirement. Cloud computing though the security barriers along with other issues need to be resolved for cloud computing to make it more viable (Marston et al., 2011). The security issues could severely affect cloud infrastructure. Security itself is conceptualized in cloud computing infrastructure as a distinct layer (Dukaric and Furic, 2013). The security threats embedded in cloud computing approach are directly proportional to its offered advantages. Cloud computing is a great opportunity and lucrative option both to the businesses and the attackers – either parties can have their own advantages from cloud computing. The vast possibilities of cloud computing cannot be ignored solely for the security reason – ongoing investigation and research for robust, consistent and integrated security models for cloud computing could be the only path of the motivation. One of the inherent problems in this content is that, the consumers might normally not be able to identify or foresee all the risks involved in the specific cloud transaction they are dealing with or involved in (Svantesson and Clarke, 2010).

Different modes of data transfer and communication means (e.g. satellite communication) might need to be taken into account. Huge amount of data transfer is a common anticipation in a cloud environment; the communication technology also becomes a security concern for the cloud computing approach. Cloud environment is associated with both physical and virtual resources and they pose different levels of security issues – having no sophisticated authentication mechanism to fully address the security threats in an existing problem for cloud computing. It has mainly resulted in the situations where grid computing has been taken as an embedded part of cloud computing (Casola et al., 2013). As the virtualized resources are highly coupled with a cloud infrastructure, intrusion related security concerns are of utmost priority as part of security issues, Lewis (2009).

Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service model employed, the operational models and the technologies used to enable cloud service, cloud computing may present different risks to an organization than traditional IT solution, Casolav et al. (2013).

In SaaS environment the security controls and their scope are negotiated into the contracts for service, service levels, privacy, and compliance are all issues to be dealt with legally in contrasts, Emman (2013).

In an IaaS offering, while the responsibility for security, the underlying infrastructure and abstraction layers belong to the provider, the remainder of the stack is the consumer's responsibility, Monjur (2014).

PaaS offers a balance somewhere in between, where securing the platform falls onto the provider, but both securing the applications developed against the platform and developing them securely, belongs to the consumer.

Cloud Computing Challenges

Despite the growing influence, concerns regarding cloud computing, it still remains and heading on. One can conclude that the benefits outweigh the drawbacks and consequently, the model of cloud computing should be explored and expanded. These challenges include: data security data recovery and availability; management capabilities as well as regulatory and Compliance Restrictions, Kim et al. (2012).

LITERATURE REVIEW

The National Institute of Standards and Technology special publication 800 – 1457 pages 4/27/2012, acknowledges the definition ascribed to cloud computing by various authors. They talked about Peter Melland Timothy Grance of (NIST) in giving credence to the various definitions. In their work Mell and Grance expatiated the essential characteristics of cloud computing which includes: on demand self-service, broad network access, resource pooling, rapid elasticity, measured service and what have you.

Microsoft private offerings at http:www.microsfot.com/private cloud explained the benefits of using Microsoft cloud and its cost benefits which highlights its cheap cost in infrastructure and software.

In Torry Harris (2012), cloud computing an overview, he highlights the realities and risks of the model, components of the model as well as the characteristics and usage of the model. This provides a means of understanding the model and exploring options available for complementing your technology and infrastructure needs.

In Alexa Huth and James Cebula (2013), the basics of cloud computing, their work laid emphasis on the cloud definition, how it is used, types of clouds and choosing a cloud provider and the security of the cloud.

In Eugine (2013) clouds' computing models, he considers the various benefits of cloud computing, the advantages and other features not known by people seeking service from providers. He also talked about potential future cloud needs, costs, security, architecture and organizational human factors that would be encountered.

Gorelik (2013), laided emphasis on economies of scale, expertise, virtualization. Commodity hardware and open source software and what it is all about. He went ahead to comment on cloud adoption and control challenges as well as the taxonomy of cloud services.

Cloud's Operations and Authentication Process

Authentication in Cloud

Security is the most prioritized aspect of any form of computing, making it an obvious expectation that security issues are crucial in cloud environment (Ashraf, 2014). Cloud computing approaches could be associated with having user's sensitive data stored both at client's end as well as in cloud servers, efficient management and authentication are very critical in cloud computing, Kings Hongs, (2012), Emmam, (2013). Verification of eligible user's credentials and protecting such credentials are part of the main security issues in the cloud. Violation in these areas cloud lead to undetected security breach, Kumar (2012). The authentication in the cloud consist of the following cloud service provider's network (ISP, firewall, router, switch, authentication server, cloud server, virtual server).

The cloud users connect to the cloud user's terminal, cloud user's terminal distributed to cloud user's ISP which distributed to the cloud. The cloud is distributed to the cloud. The cloud is distributed to the cloud service providers network which collaboration through cloud to the Authentication Management provider. Figure 1 illustrate the operation of the cloud and its authentication.

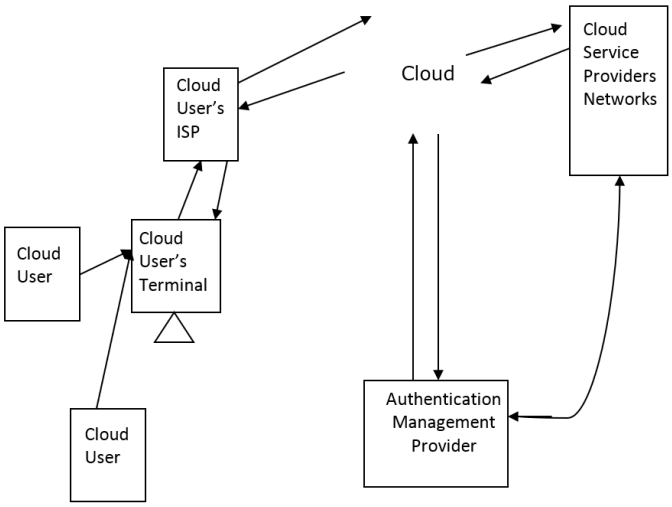


Fig. 1: Diagram of the operation of cloud and its authentication

DISCUSSIONS

Cloud computing is a new dimension in the distribution of computing services through internet connection. This type of computing services was not available at the incipiency of computing technology. Most people who are subscribing to cloud service do so considering its functionality, benefits and economics of scale. The cost of hardware and its maintenance makes it difficult for most organizations with little capital investment to invest in cloud infrastructure, especially the cloud software which is subject to critical security manipulation. We have various platforms in the services offered by cloud providers: this ranges from Private, Public and Community clouds, Yesin A. et al. (2012).

Despite the growing influence of cloud computing, there are concerns regarding the service in the areas of: data protection which involves security of data. Consequent upon the current cyber-crimes and indiscriminate hacking of websites, the protection of clouds is undoubtedly critical. The service providers are responsible for the security of the cloud.

In the area of data recovery, operational teams support, appropriate clustering, data replication, system monitoring and maintenance, disaster recovery as well as capacity and performance management. If any of these services goes below the expected standard, it could bring serious damages and

impact to the provider. The analysis of cloud computing models has shown that public cloud model is likely to stay dominant and keep expanding in the market. But the Private and Hybrid deployment models are going to stay ahead and market shares will continuously drop due to the difficulty of increasing infrastructural costs as well as software costs. By and large these group- Private and Hybrid models eventually will be used for specific business purposes, Kumar A. (2012).

CONCLUSION

The emergence of cloud computing has brought a distinctive means of doing the business of information technology. The process has continued to expand as the providers apply various technological innovations. With many companies entering the cloud service business, and the innovations that are used, the market share spreads and only those with sophisticated and current technology in areas of hardware infrastructure and software technology resistant to the ongoing cybercrime will dominate and have a good market share. The use of open source software is no longer in vogue as this system was used by new entrants into the cloud services. But major players in the market use proprietary systems, with proprietary sophisticated technologies to gain competitive advantage. Companies like (Hp) is using open source software just because they are new entrants, but companies like: Amazon, Google and Microsoft that have been well established in cloud business are the ones that use proprietary technology. We shall see where the business of cloud would take us in the near future.

REFERENCE

1. Kim, J. and Hony S. (2012). A consolidated Authentication Model in Cloud Computing Environment. International Journal of Multimedia and Ubiquitous Engineering.
2. Monjur, A. and Mohammad, A. (2014). Cloud Computing and Security Issues in the Cloud "International Journal of Network Security and its application.
3. Emman, A.H.M. (2013). Additional Authentication and Authorization using Registered E-mail – ID for Cloud Computing. International Journal of Soft Computing and Engineering, 3(2), 110-113.
4. Han, J., Susilo, W. and Mu, Y. (2013). Identify – based data Storage in Cloud Computing. Future Generation Computer Systems, 29, 673-681.
5. Yassin, A.A., Jin, H., Ibrahim A., Qiang, W. and Zou, D. (2012). Efficient Password – based two factors Authentication in Cloud Computing. International Journal of Security and its Application 6(2), 143-148.
6. Kumar, A. (2012). World of Cloud Computing and Security. International Journal of Cloud Computing and Services Sciences, 1(2), 53-58.
7. Dukaric, R. and Juric, M.B. (2013). Towards a Unified Taxonomy and Architecture of Cloud Frameworks. Future Generation Computer Sytems; 29, 1196-1210.
8. Casola, V; Euomo, A; Rak, M. and Villiano, U. (2013). The Cloud Grid Approach: Security Analysis and performance evaluation. Future Generation Computer Systems, 28, 85-93.
9. Florin, O.N. (2012). Cloud Computing Security Issues: Journal of Defense Resources Management Vol. 3, Issues 2(5) 2012.
10. www.cloud.standard.org
11. Reese, George (2009). Cloud Application Architectures: Building Application and Infrastructure in the cloud, O'Relty Media.
12. http://aws.amazon.com/documentation/getstarted
13. http://www.gogride.com
14. http://www.rackspace.com
15. Lewis, Grace (2009). Cloud Computing: Funding the Silver Lining, not the Silver Bullet, http://www.SEI.cmu.edu/library/abstract/white-papers/cloudcomoutingbasics.cfm
16. Jasen Wagne and Grace Timothy (2011). Guidelines on Security and Privacy on the Cloud Computing. National Institute of Standards and Technology.
17. Strowd, Harrison and Lewis, Grace; T-check in system-of systems technologies: cloud computing. (cmu/SEI-2010-TN-009). Software Engineering Institute Carnegie Mellon University. http://www.SEI.cmu.edu/library/abstract/reprots.
18. Eugine, Gorelik (2013). Cloud Computing Models, Masters Thesis, MIT Sloans School of Management and MIT Engineering Systems Division Boston Massachusetts U.S.A.
19. Parklick D. (1966). The Challenge of the Computer Utility. Addition Wesley Educational Publisher