IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. II (Sep – Oct. 2014), PP 57-61
www.iosrjournals.org

Security Challenges of Cloud Computing For Enterprise Usage and Adoption

Folusho Abayomi Oyegoke
ICT Department,SAIPEM Contracting Nigeria Limited, New Operational Base,
Port-Harcourt, Nigeria.

Abstract**:** *Cloud computing has brought about a paradigm shift in Information Technology services globally most especially in developed countries for mid-sized to large scale enterprises. It has emerged as one of the major IT trends of the 21st century. Cloud computing simply refers to the process of storing and accessing data and applications over the internet in a remote location instead of the localhard drive storage. This has brought about so many advantages in business and has helped improved productivity in the organization; cost-efficiency, scalability, easy access to information, unlimited storage and flexibility are also some of the benefits. However, several challenges abound with the use of cloud computing. Despite the numerous benefits it offers, Security threats and risk stands out as a major constraint for organizations. This paper examines some of the benefits of cloud computing and the challenges in the enterprise environment and factors militating against its full adoption.It focuses more on the security challenges that includes data protection, privacy, security standardsas well as network attacks.*

Keywords**:** *Cloud Computing, Enterprise, Information and Communications Technology (ICT), Security threats, Cloud Service Providers (CSPs), Enterprise Cloud Computing.*

I. Introduction

The term "Cloud Computing" was first academically used by Professor Ramnath K. Chellappa in 1997 [1]. He defined it as "a computing paradigm where boundaries of computing will be determined rationale rather than technical limits" [2]. For most users and people, cloud computing simply refers to the ability to have files and data stored in a remote server typically know as a Cloud service providers (CSPs) instead of their local hard-disk or storage devices. Examples of CSPs include Microsoft, salesforce.com, Amazon, Google, etc. These services can be accessed from any computer or device that is connected to the internet 'cloud' as a host. Users are able to upload their data and retrieve it whenever they log in with their access. The National Institute of Standards and Technology (NIST) special publication (2011) defined Cloud computing as 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 [3]. The term 'cloud' is synonymous with the internet. As depicted in figure 1, it encompasses all IT services ranging from applications, platform, infrastructure, database, storage, collaboration, network, etc. With the ubiquitous nature of IT, the cloud has offered a more promising future for home users, mid-scale and large enterprises alike. Enterprise cloud computing is therefore a special case of utilizing cloud computing for the competitive advantage through breakout opportunities both for cost savings and more importantly, for business innovation in terms of unprecedented speed and agility with vast improved collaboration among business partners and customers [9]. The 2012 Global Cloud Computing Survey Results reported four major advantages of enterprise adoption; they are Administration, Cost, Partnership and Data [8]. In terms of administration, it provides for easier software access, disaster recovery and enables rapid deployment. For Cost, it requires a very low capital investment from the enterprise and also requires fewer IT personnel thereby transforming capital expenses into operating expenses. The Partnership benefit improves collaboration between different enterprises whether in a project or contract. In terms of data, it improves data security creates room for better data organization and puts them under control.

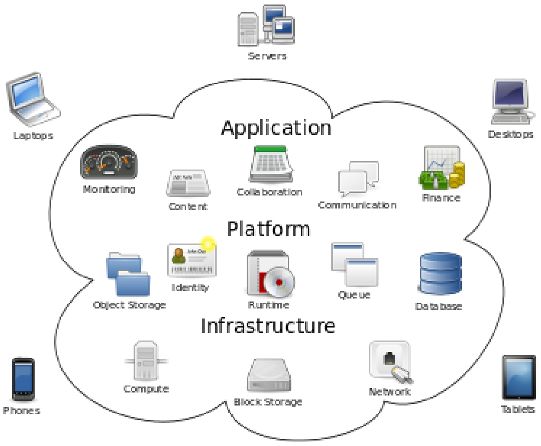


Fig. 1: A logical diagram of Cloud Computing [4].

II. Related Works

MajadiNazia [5] investigated the security issues and challenges of cloud computing focusing on the types and service delivery types of cloud computing. Parekh Disha& R. Sridaran [6] in their paper examined different security threats under the cloud model as well as network concerns to stagnate the threats within cloud. Though most of the existing research discusses cloud computing security, they focused more on the model types and did not relate it to the challenges of enterprise usage and adoption in the contemporary context. In 2012, UgochukwuOnwudebelu& Benedict Chukuka [7] researched about the adoption of cloud computing by the enterprise and the risk involved. They tried to expose potential sources of risk that an enterprise may face as it become a member of the cloud initiative world. They highlighted four main sources of risk which are Enterprise Risk, Technical Risk, Legal Risk and Common Risk that an organization may be confronted with as it embark to join the cloud world. It however did not examine the different security challenges enterprises may encounter from the total implementation of cloud computing.

III. Models Of Cloud Computing

Cloud computing have three well known service models. These are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). SaaS is a software distributionmodel in which applications are hosted by a service provide and made available over a network to customers. Its main purpose is to reduce the total cost of hardware and software development, maintenance and operations. In SaaS, security control is carried out mainly by the cloud provider [12]. Cloud computing has changed how enterprise applications are built and executed. Platform-as-a-Service (PaaS) is a proven model for running applications without the stress of maintaining the hardware and software infrastructure at your company. PaaS removes the expense and complexity of evaluating, buying, configuring, and managing all the hardware and software needed for custom-built applications [14]. Infrastructure as a Service (IaaS) is also a model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis [15].

IV. Benefits Of Cloud Computing For Enterprise Usage

Basically, the overall benefits of cloud computing can be summed up into the following categories; to reduce cost (savings), ease of access (accessibility), efficiency and flexibility which results to improved productivity and innovations.As seen in Figure 2 [16], cloud computing has so much more benefits and advantages to enterprise thatit is difficult to resist. In terms of saving cost, it has reduced the cost of IT infrastructure hardware and resources used by the enterprise. All these are the responsibilities of the Service Providers. The enterprise need not to worry about power to run these infrastructures also. Another benefit is Scalability; the enterprise only needs to pay for the applications and data storage used. This can be referred to as “Pay-as-you-go” system. Consider an enterprise moving from one location to another. The continuous availability means that public cloud services are available wherever the enterprise is located.

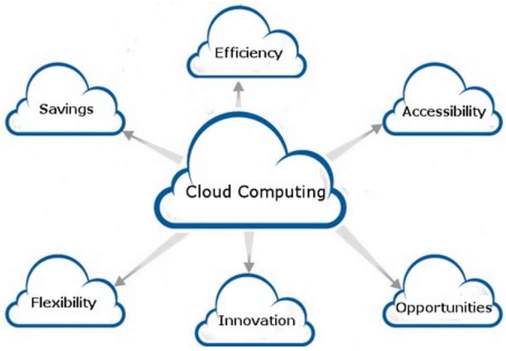
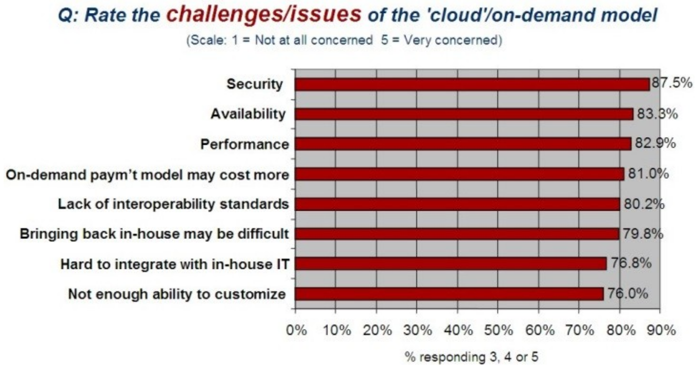


Fig. 2: Benefits of Cloud Computing [16]

V. Major Challenges Of Cloud Computing

Loopholes and risk are associated with all modern technologies. Inasmuch as the benefits of cloud computing, there seems to exist some challenges associated with it. These challenges are contributing factors preventing organizations from adopting and using this technology. The IDC 2010 survey ranking of cloud computing security challengesranks 'Security' as the top concern as depicted in Figure 3. Other challenges include Availability, Performance, On-demand payment model may cost more, lack of interoperability standards, bringing back-in house may be difficult, hard to integrate with in-house IT and not enough ability to customize.



Source: IDC Enterprise Panel, 3Q09, n = 263

Fig. 3: Results of IDC survey ranking security challenges, 2010 [4].

VI. Security As A Major Challenge

The Cloud Computing Adoption Survey 2011 clearly portrays some of the security concerns that affect the usage by enterprises. As depicted in Figure 4, Data security is a major issue with information leakage and compliance and audit trails of primary concern. Other Security concerns include; (i) ensuring data destruction on infrastructure we do not own, (ii) Lack of security standards among cloud providers, (iii) OS Security, (iv) Network security, (v) Data portability, (vi) Not knowing where my data resides, (vii)Identity and access management and (viii) Data more prone to attacks when several companies' info is hosted in one place.

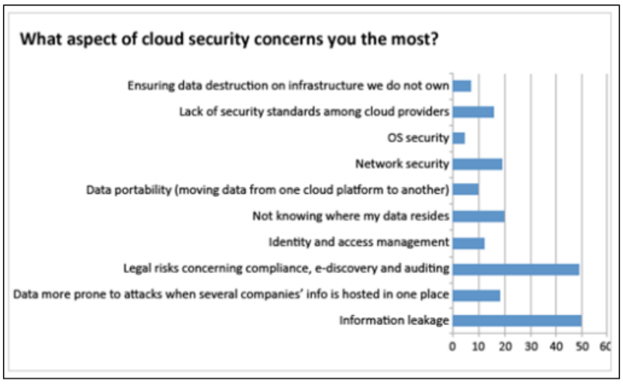


Fig. 4: Results of Cloud Computing Adoption Survey 2011 [10].

A. Ensuring data destruction on infrastructure we do not own

If an organization determines to move from one CSP to another, it probably must move its files and data too. How then will it ensure that the enterprise files and data on the previous cloud have been fully destroyed? Roberts (2014) suggested some ways by which cloud data can be gotten rid of. The first method could be done by the use of a random bit pattern. Most CSPs have a data destruction policy which overwrites all the disk data previously used by a customer. For IaaS (Infrastructure-as-a-Service), data can be overwritten by using some Linux and Windows programs that follow the NIST protocol. Monica et al (2014) described the Time constrained data destruction in cloud [11]. The time constrained data system is used to meet all the privacy-preserving goals. This can be referred to as Data Self-Destruct. Despite these data destruction technologies, there exists some data recovery software that can recover files from the cloud services. For example, Kroll Ontrack has recovered data from many cloud storage providers whose clients did not have any backup redundancy [19]. This is a concern to enterprises about their data even after they have switched to another CSP.

B. Lack of Security standards among cloud providers

According to Aaron Weiss, 2013 [17], A confusing collection of cloud security standards can make it tough to evaluate cloud provider security. When enterprises maintain their own IT in-house, they can define and control the security standards and protocols to suit them. When using a Cloud Provider or a third party then the security standards they apply have to be known by the client enterprise. Even though the Cloud Security Alliance (CSA) which is the largest and most comprehensive player in the cloud security standards has developed a compliance standard, it has not been fully adopted by most Providers especially in Asia. For example, in Japan, the Ministry of Economy, Trade and Industry has developed a cloud security standard to be followed by providers in the country. The International Organization for Standardization, or ISO, plans to draw up a final draft of security standards for cloud computing in April 2015, and new international standards are expected to take effect in October that year. Japan, the U.S., the U.K., Australia, Asian nations and others have already basically agreed that the new standards will be based on Japanese guidelines [18]. Until the finalization and unification of these security standards among cloud providers, there will still be a level of skepticism for enterprise adoption. Even though various providers have their own standards, there ought to be a standard security policy in place.

C. Operating System and Network Security

Enterprises and various organizations use the cloud for different services. Either for Software, Platform or Infrastructure as a Service,all these services are connected from the Service Providers to the user via a network which is most probably the internet. Also the users within the enterprise access the cloud using an Operating system. What guarantee can the cloud provide for enterprises that use these services? Ordinarily, traditional In-house data centers have in place some network security measures within the LAN (Local Area Network) which includes but not limited to the use of security infrastructure like Firewall, VPN, Access-lists, Intrusion Detection System (IDS) etc. With enterprise data and services running on the Cloud, the security of the network against intruders and hackers is therefore a major point of concern for any organization. This has led to the concept of “Cloud Security”. Some enterprises are worried and concerned about the threats involved with the traffic of millions of megabyte of data over the internet daily.

D. Data more prone to attacks when several companies’ info is hosted in one place

We are aware that storing of information in the cloud could make a company susceptible to external hackers. For example if a Credit card company uses a particular CSP, it will be more prone to attacks from hackers. It therefore means that if a provider is attacked then other clients whose services are hosted alongside with the targeted victim might be jeopardized. It can even lead to a shutdown of the services and data loss.

E. Identity and access management

Enterprise needs to manage access to information and applications scattered across various (internal and external) application system. They must provide this access for a growing number of identities, both inside and outside the organization, without compromising security or exposing sensitive information [13]. Identity and Access Management usually referred to as ‘IAM’ comprises of four main parts; Authentication, Authorization, User management and Central User Repository. The sole aim of IAM is to provide the right people with the right access at the right time. As more and more organizations add more cloud services to their infrastructure, the process involved in the managing of identities is getting complicated. This is a serious challenge that enterprise worry about when moving to the cloud services. Poorly controlled IAM process could result to identity theft and unauthorized access to files and services.

VII. Conclusion

There is no doubt that Cloud computing is a technology for the future and has come to stay. In this paper, I have examined briefly some of the benefits associated with cloud computing as well as some security challenges especially in the enterprise environment. While some enterprises have fully implemented cloud computing, others are unassertive about its usage and adoption. This is due to some of the challenges highlighted in this paper.There is however hope that these challenges will be mitigated to enable them adopt and use Cloud computing services to achieve the desired result and productivity.

References

[1]. Wikipedia. (2012, December 5). Mobile Cloud Storage.[Online].Available: http://en.wikipedia.org/wiki/Mobile_Cloud_Storage

[2]. Cloud computing(2014) [Online].Available: http://www.contrib.andrew.cmu.edu/~madhurim/cloud%20computing.html

[3]. P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” IT Laboratory NIST., Gaithersburg, MD, Tech. Rep. 800-145, 2011.pp.1-3.

[4]. Enterprise Cloud Computing: Transforming IT (2009, July).[Online]. Available:http://www.inst-informatica.pt/servicos/informacao-e-documentacao/dossiers-tematicos/teste-dossier-tematico-no-7-cloud-computing/tendencias/enterprise-cloud-computing-transforming-it

[5]. N. Majadi. “Cloud Computing: Security Issues and Challenges” The International Journal of Scientific & Engineering Research, vol.4(7), pp.1515-1520, Jul. 2012.

[6]. D. Parekh and R. Sridaran. “An Analysis of Security Challenges in Cloud Computing” The International Journal of Advanced Computer Science and Applications. vol. 4(1), pp. 38-46, 2013.

[7]. U. Onwudebelu andB. Chukuka. “Will Adoption of Cloud Computing Put the Enterprise at Risk?” 2012 IEEE 4th International Conference on Adaptive Science & Technology (ICAST),vol. 1,pp. 82-85, 2012.

[8]. 2012 Global Cloud Computing Survey Results (2012, September). [Online]. Available: http://www.techsoupglobal.org/2012-global-cloud-computing-survey

[9]. M. Rouse, (2010, December). What is Cloud Computing? [Online]. Available: http://whatis.techtarget.com/definition/Enterprise-Cloud-Computing-FAQ.

[10]. M. Laverick. (2010, June 5), Cloud computing adoption remains tepid. [Online].Available:http://www.computerweekly.com/news/2240036468/Cloud-computing-adoption-remains-tepid.

[11]. S. Monica and M. Subasini, “Time Constrained Data Destruction in Cloud”,TheInternational Journal of Innovative Research in Computer and Communication Engineering, vol. 2, pp. 1246-1254, Mar. 2014.

[12]. W. Jansen and T. Grance, “Guidelines on Security and Privacy in Public Cloud Computing” IT Laboratory NIST., Gaithersburg, MD, Tech. Rep. 800-144, 2011. pp. 1-52.

[13]. What is Identity and Access Management? (2014). [Online]. Available: http://www.karingroup.com/eng/about/what_is_identity.pdf.

[14]. What is Platform as a Service (PaaS)? (2014).[Online]. Available:http://www.salesforce.com/paas/overview/.

[15]. M. Rouse. (2010,August).Infrastructure as a Service (IaaS).[Online]. Available:http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS.

[16]. Fiscal Benefits of Cloud Computing For Nonprofits (2013, November 25). [Online] Available: http://blog.techimpact.org/2-fiscal-benefits-cloud-computing-nonprofits/.

[17]. A. Weiss. (2013, March 12). Cloud Security Standards: What You Should Know.[Online]. Available: http://www.esecurityplanet.com/network-security/cloud-security-standards-what-you-should-know.html.

[18]. Japan's cloud security rules set to become global standard. (2014, March 14) [Online]. Available: http://asia.nikkei.com/Politics-Economy/Economy/Japan-s-cloud-security-rules-set-to-become-global-standard.

[19]. Cloud Based Data Recovery (2014) [Online]. Available: http://www.krollontrack.co.uk/data-recovery/data-recovery-services/cloud-data-recovery/.