The Fear and "Phobia" of the Cloud and Cloud Computing

Arthur Ume

School of Information Technology and Communications
American University of Nigeria, Yola, Nigeria

Abstract

Cloud computing is a rapidly evolving innovation that offers the potential for businesses to gain competitive edge globally. With the advent of Cloud computing, organizations may easily port and render their businesses, services and operations across the globe via the Internet. This huge possibility looks very attractive, and increasingly many enterprises in the developed economies are beginning to think of how to leverage this opportunity; with Cloud computing, services and data may be provided by shared computing resources in scalable data centers and made accessible over the Internet. Nevertheless, there is still a predominant and nagging fear (phobia) surrounding the adoption of the easy-to-manage offerings of the Cloud computing technology, especially in developing countries like Nigeria.This paper gives a general insight into Cloud computing and its history. It then attempts to investigate why businesses tend to shy away from the use of the services which can/may be rendered in the Cloud. It further discusses the prospects of extensively introducing and leveraging Cloud computing as a means of rendering distributed business operations and services in a cost effective way especially in developing sectors of developing economies like Nigeria where organizations and companies may not be all that economically buoyant to own and build their own individual "silo technologies" to attend and solve crucial business needs. Finally the paper suggests how to start overcoming the in-built and inherent resistive attitudes towards Cloud computing.

Keywords: *Cloud computing; phobia; silo technologies,distributed business operations and services*

Introduction

Cloud computing according to Dave Cleveland (2012) is a technology that uses the Internet alongside the central remote servers to maintain data and application. In other words, it is a technology that allows users to share files and applications over the Internet including storage.

Cloud computing is one of the recent innovations in distributed computing technology. There has been a tremendous increase in its application and use in the computer world. As a result of this, its vulnerabilities should be well inspected and deduced.

The name Cloud computing is gotten from the Cloud symbol used to represent the Internet in flowchart diagrams (IBM, 2007). The underlying concept of Cloud computing dates back to 1960 when John McCarthy (an American computer scientist) opined that, "computation may someday be organized as a public utility" (Eric, 2008). Further researches on Cloud computing have been carried out from that time until Microsoft, IBM, and Salesforce started exploring the full application of Cloud computing in early 2000 (Miller 2011). According to Micheal, (2010) Cloud computing can be defined "as the applications provided as services over the Internet and also the hardware and systems software in the data hubs that make available these services." Simply put, Cloud computing replaces software applications or documents used by offices or businesses with servers elsewhere

and can be accessed via the Internet. This means that there exist data centers that contain several servers accessed by customers form different areas.

In the next section of this paper, the authors describe the various types of services which can be rendered through Cloud computing.

Services of Cloud Computing

- Software as a Service (SaaS): This is a software delivery service that provides access to different computing software on the web. Eric (2008) explains that SaaS delivers a single application through the browser to thousands of customers using a multitenant (multiple customers using the same public Cloud) architecture. A popular example of this service is the Google doc or Gmail which provides access to word processing and email services in the Cloud. No document or email is stored locally and these documents can be accessed from anywhere (Miller, 2011). In this platform companies can share and access all the software delivery models remotely via web based Internet. This implies that such applications are run virtually through virtual servers and paid for as per their use. The service is usually provided through some type of front end or web portal. While the end user is free to use the service from anywhere, the company pays a per use fee.
- Platform as a service (PaaS): PaaS is another popular service which is offered by Cloud computing. It is often seen as a variation of SaaS. As the name conveys, Platform-as-a-Service area of Cloud computing offers developers a medium through which they can create and develop software applications virtually. All the content management systems like Joomla and WordPress are platforms that are usually pre-configured open CM systems, which allow IT professionals to develop software applications remotely. An example of PaaS is GoogleApps. With PaaS, software development environments can be made available on the Cloud for use. PaaS providers use APIs, websites portals or gateway software installed on the customer's computer (IBM, 2007). An example of PaaS Clouds is "Force.com." Force.com is a Cloud computing system provided by Salesforce. It is used by developers to build and deliver applications, it is a platform where multiple customers can use an application offered on the server (Cloud) for service (Miller, 2011). Other providers of PaaS include Microsoft's Azure, Google Maps, ADP Payroll processing, and US Postal Service offerings.
- Infrastructure as a service (IaaS): The infrastructure of any company comprises of hardware, software, networking components, servers, and storage space. With Cloud computing IaaS platform, a company cannot only get the devices independently but can also enjoy working in the virtual world. This model is similar to a utility company model, IaaS allows a company to pay for only as much capacity of data as needed. It provides more space when necessary. An example would be when a Shop is on sales and the managers wish to expand their capacity to avoid crash from overload. The company can expand the size and then undo the size change after the sales peak period is over. An example of a site that uses IaaS Cloud is Amazon (Michael, 2010).

Benefits of Cloud computing

There are lots of benefits in using Cloud computing in to render or access computing resources. Presently a lot of people use Cloud computing without even knowing what it means. For example, Gmail, Yahoo mail, YouTube, and Skype users…are all in the Cloud. The layman probably does not

care to know what exactly is happening when he goes to check his mails. Increasingly companies and organizations are becoming aware of the huge benefits that Cloud computing provides. The next section of the paper outlines some of these benefits.

- Flexibility and storage: With Cloud computing Files are stored in the "Cloud". This allows for development in the organization because workers no longer have to worry about the storage of documents. Also, workers can access office files from wherever and whenever. Workers can also work together virtually even when they are not at the same place at the same time. Various documents can be viewed simultaneously provided Internet connection is available (Arno, 2011).
- Time saving: Alongside easy collaboration, Cloud computing also aids the easy access to information. Easy access in this context could be seen in how fast it is to access Gmail, Yahoo mail, mailboxes in general. It is fast and easy in contrast to the time it would take to download and install software (Arno, 2011).
- Reduced Cost: Cloud computing puts a stop to the illegal reproduction and distribution of software. (Hinchcliffe, 2009) states that, with Cloud computing, payment is made for only software used. Some software on the Cloud is free. For example, most SaaS solutions have a pay-as-you-go pricing model instead of a large up-front investment. Such pricing models allow end users to pay only for what they use thus freeing up resources such as time and money for other more important (core) business activities (Hinchcliffe, 2009). For example, the Salesforce Company charges from five US dollars to twenty five US dollars per month for its services. Implementation of Cloud computing will reduce the investment cost in server hardware and software licensing. Cloud computing is therefore cheaper and less labor intensive for companies. There is no need to buy and install expensive software. There is no need to acquire, track and manage software licenses.

The Persisting Fear and "Phobia" around Cloud Computing

Despite the benefits enumerated above, it is surprising that not many companies and organizations are rushing to leverage the advantages of Cloud computing, especially in developing countries. Through observations, the authors tried to unravel the reasons for the persisting apathy.

It is true that Cloud computing today is presently one of the most captivating technologies of our time, but it is also the most feared. Although there are a lot of benefits of Cloud computing, many individuals and organizations still have their reservations about this innovation. The authors observed that the most talked about issue of Cloud computing is security. As (Kuyoro, Ibikunle and Awodele, 2011) rightly noted, with Cloud computing, users feel that they are not given any assurance of safety; they argue that a Cloud platform which has the ability to satisfy their requirements needs to be more convincingly and persuasively safe.

(Anna, 2011) wrote that the fear of Cloud computing has left users wondering and going in circles. There is no trust and users expect their information to be safe. She opined that this fear may just be as a result of ignorance on the part of the users; she further pointed out that Microsoft is known to have various data centers located across the globe. These data centers back up each other so that if data is lost or affected, data is replicated. For example, Microsoft guarantee 99.9% financially backed uptime for their customers because they have full confidence on their services. So, the figment of security implications may not be real, but an illusion in people's heads.

The next part of this section of the paper discusses the specific challenges and envisaged limitations which are serving as the major causes of the fear of Cloud computing in a typical

developing economy with developing sectors. For the purpose of this paper, the observed security challenges of Cloud computing in Nigeria as typical developing country will further be highlighted.

Privacy

Privacy is a vital concept in the world of Information and Communications Technology. Cloud computing basically refers to entrusting a company's data to systems managed by companies on remote servers. As (Miller, 2011) rightly pointed out, there are serious privacy and confidential issues involved when talking about Cloud computing. The companies entrusted with customer information and data have constant access to them and can accidentally or intentionally reveal it or utilize it for unauthorized purposes. This is why most users have a second thought when considering Cloud computing.

(Pardeep 2011) also points out that the Privacy statements written by Cloud providers are written in very complicated ways and are not understood by their customers. Customers, bored away by the complex terms, agree to the terms of service and hand over their personal information and data to these Cloud providers. He further predicted that Cloud computing will be the wave of the future but the massive availability of data and resources within a Cloud will be a very attractive target for hackers. This he said would continue to serve as a main drawback of Cloud computing. The authors' observations in the sectors of study in Nigeria also echo these reservations.

Data Availability

Data availability is one of the key requirements users expect from any software or computing technology. Most times, customers want to move around with their data. For example, most people would store their personal data such as pictures in an eight gigabytes or sixteen gigabyte memory chip and carry it around. Whenever the need to view pictures arises, they can plug in the memory chip into a camera and view/use the pictures or images. In the vast cities of Nigeria, the problem with availability in Cloud computing is that, when there is no Internet access or connection, it is the same thing as a denial of service attack. The prevailing electric energy crisis in Nigeria is not helping this negative assumption among computer-literate work force.

This problem was also captured by (WHSR, 2012). As much as Cloud computing serves as a good storage device, it is not readily available, especially in the case where network service is not assured. A country like Nigeria without constant Internet will be at a disadvantage as long as this status quo prevails.

Traditional security

Traditional security enumerates computer and network attacks that will be faced by moving to the Cloud. Pardeep, (2011) explains that the security issues of Cloud computing stems from the fact that the platforms used in integrating Cloud applications are not securely created. Even the infrastructures used to connect and interact with the Cloud (servers) are not fully secured. He opines that this is because, the knowledge of authentication and authorization of Cloud programs have not been fully explored. (Anna, 2011) also points out to another security issue which arise from the fact that in order to effectively search through the data in the Cloud it requires un-encrypting it - which gives the Cloud provider and possible hackers an access to the data. Cloud providers may try to tackle these concerns by arguing that their security measures and processes are more developed and tested than those of a regular company. They may also argue that it may be easier to enforce

security through contracts with online services providers than through internal controls (Pardeep, 2011). As Cloud computing continues to make headway, new security issues are surfacing. Some of these security problems are discussed further in the following paragraphs:

Although the Cloud computing infrastructure is generally very secure, it is impossible to be completely certain that security issues will not arise. Cloud computing providers particularly the SaaS and PaaS providers, are constantly bragging about the capabilities of their systems offerings. They often claim that their Cloud security is tighter than those of other enterprises. The issue is that among the computer-literate populace in most developed countries, it is a known fact that security systems that have been breached once are somehow unreliable. It is common knowledge that such reputable companies as Google and Salesforce have faced security breaches and issues in the past, and therefore users cannot be completely certain that it will not repeat itself (Banerjee, 2012).

During their observations and discussions the authors found out that this issue and notion is even more prevalent and adamant among the computer-literate work-force and stakeholders in Nigeria's developing sectors and economy.

Another key quality assurance and security issue which prospective providers, customers or users of the Cloud computing resources and technologies may face in countries like Nigeria is that unlike many companies operating in the US, Canada, or the European Union there are in existence a standardized regulatory requirements that providers must abide by (e.g., ISO 27002, Safe Harbor, ITIL, and COBIT). Every company which is a Cloud provider is expected to meet these requirements, and should be ready to go through all certification, accreditation, and review. Unfortunately, observations indicate that in developing countries like Nigeria, these standardized regulations are not yet adhered to by most software companies.Prospective beneficiaries of Cloud computing still think that they would still be ultimately responsible for the integrity and security of their data regardless of the fact that it is held by a Cloud service provider.

Prospective customers interviewed by the authors do not trust that their company data and business processes would be handled adequately. To deepen this apprehension, when making use of the Cloud, users are not usually aware of exactly where their data is hosted. In most cases, data is not stored in the same country as the users. Users then have to confirm or request that their data be stored in specific jurisdictions (Banerjee, 2012). The authors of this paper observed this to be more so among the teeming population of new visitors to ICT (Information & Communication Technologies) in the country of study.As observed by (WSHR, 2012), Cloud services are known to be very difficult to investigate. This is because activities of various users may be co-located and spreads across various hosts. Therefore if criminal activities are taking place using the Cloud, it will be difficult to trace or just impossible to pinpoint.

Though some of the basic security issues such as loss of data, phishing, including some of the issues discussed above are beginning to have some sort of solutions attached to them, regardless of the fast growth of Cloud computing, it is still evident that security issues and apprehension are still stunting the extensive acceptance of Cloud computing even in countries with developed economies.

Cloud Computing among Enterprise Organizations in Nigeria's Developing Sectors

At present only a few organizations and businesses are willing to outsource applications that involve less sensitive information. According to a survey of more than 50 chief executives and IT managers of 10 companies conducted in key State capital cities of Nigeria, companies and enterprises would still trust and prefer their existing internal systems over Cloud-based systems for the foreseeable future. This is due to the fear for loss of control of key data, core business processes

and systems. The ones that do agree to consider the Cloud demand thorough third party risk assessments; they would only do so experimentally with just one or two of their peripheral business offerings or process. All the respondents' worry, apprehension and noticeable uneasiness can be translated into what can be identified as the main obstacles to the adoption and growth of Cloud computing in a developing country.

Permanent solutions to this predominant apathy towards Cloud computing seem nebulous. It is important for prospective providers to first of all embark on providing extensive company-level orientation training for prospective users to understand what Cloud computing really means. Google is presently embarking on such subsidized extensive orientation and training at Lagos, Lagos and at the American University of Nigeria, Yola.Apart from these company-level orientations, prospective users should be helped to get acquainted with the privacy statement involved with all aspects Cloud computing. Users should be aware of the data or information collected from them and as such, users will be able to know the level of security they require.

Moreover, Pardeep (2011) notes that if users want their data to be secure, there is a need to let them encrypt their stored data. The encryption keys should not be stored on the same server. According to (Michael, 2008), the reliability of the Cloud computing platform provider should also be a major concern, and should be emphasized before customers choose to patronize the Cloud computing offering. A reliable provider of Cloud computing platform should assure users of a certain percentage of data security. Further, it is necessary for back-ups of customer's data to be kept in cases of system failure. The back-up file should be kept in a separate location from the original without any fear of security breach. In the aspect of data availability, in order to tackle the issue of Internet connection, companies that patronize Cloud computing need to purchase several network servers. Relying on one Internet server is not appropriate in times of network failure.

Specific Solutions

There are several groups interested in developing standards and security for Cloud computing and Cloud security. For example, the Cloud Security Alliance (CSA) is encouraging solution providers, non-profits and individual companies to enter into discussion about the current and future best practices for information assurance in the Cloud. The Cloud Standards web site is collecting and coordinating information about Cloud-related standards and security assurance under development by other groups. The Open Web Application Security Project maintains a top 10 list of vulnerabilities to Cloud-based computing as Service deployment models. These are being updated as the threat landscape changes. In the next paragraphs the paper will go through some of these solutions.

Web Application Solutions

The best security solution presently researched for web applications is the possibility to create a development framework that shows and teaches a respect for security. Talks of putting forth a four-tier framework for web-based development are ongoing; this implies a security facet in the process. Also the X10 language is looked at as one way to achieve better use of the Cloud capabilities of massive parallel processing and concurrency.

Accessibility Solutions

Here, researchers are pointing out the value of filtering a packet-sniffer output to specific services as an effective way to address security issues shown by anomalous packets directed to specific ports

or services. An often-ignored solution to accessibility vulnerabilities is to shut down unused services, keep patches updated, and reduce permissions and access rights of applications and users.

Authentication Solutions

A researcher (Basta, 2007) suggested one way to avoid IP spoofing by using encrypted protocols wherever possible. He also suggests avoiding ARP poisoning by requiring root access to change ARP tables; using static, rather than dynamic ARP tables; or at least to make sure changes to the ARP tables are logged.

Data Verification, Tampering, Loss and Theft Solutions

In this regard, (Hayes, 2008) points out that there is no way to know if the Cloud providers properly deleted a client's purged data, or whether they saved it for some unknown reason.Talks are around the possibility of employing resource isolation to ensure security of data during processing, by isolating the processor caches in virtual machines, and isolating those virtual caches from the Hypervisor.

Privacy and Control Solutions

A feeling of absolute security or control is relative. The issues of privacy and control cannot be completely solved in absolute terms, but can be assured with tight service-level agreements (SLAs) or by trying to keep the Cloud itself private. This will always point out a persisting wrinkle, because allowing a third-party service to take custody of personal/company documents raises awkward questions about control and ownership: If one moves to a competing service provider, can he/she take a data with him? Could he/she lose access to a document if he/she fails to pay a bill (Hayes, 2008)?

Conclusion

Despite its great appeal, for developing countries, Cloud computing may still not be the best option for all types of businesses or offices. Its usefulness depends on the size of company, line of business and level of incorporation of Information and Communications Technology. Cloud computing may proof to be a better option for most businesses down the line. Indicators show that more people are beginning to understand what it entails, how it works and its usefulness. But still, the fear (phobia) of surrendering absolute control of core business operations and processes to the Cloud still remains a nagging issue that will only go away in the future. Executive managers and business stakeholders interviewed and observed by the authors of this paper all indicate this attitude.

Hopefully, this fear of the Cloud will become a thing of the past as increasingly computer technology-literate managers are starting to give serious considerations to the cost and labor saving incentives and advantages this innovation may offer. In response to the crucial need to securely store, manage, share and analyse large amounts of complex data, it is of great importance that Cloud's big organizations like the Google continue to show that the Cloud can indeed be secure.

Although this is true, it will be extremely difficult to provide a complete solution to securing the Cloud in relative terms thereby completely erasing the anxiety and disquiet which the idea of outsourcing key and crucial business operations, and technology may create. Security measures

such as data encryption should be advised and employed by end-users to reduce the fear and risk of data invasion. If the phobia about security problems of Cloud computing are addressed, Cloud computing will revolutionize the world of information technology, even in developing countries Cloud computing promises real benefits to companies seeking a competitive edge in today's economy. Attractive pricing, the ability to free up staff for other duties is beginning to drive businesses to consider Cloud computing.

References

Anna. (2011, December C). The Fear of Cloud Computing. Retrieved April 20, 2012, from http://www.axon-it.com/2011/12/06/the-fear-of-Cloud-computing/

Arno, C. (2011, August 14). The advantages of using Cloud computing. Retrieved April 29, 2012, from http://Cloudcomputing.sys-con.com/node/1792026

Banerjee, U. (2012, April 27). Gartner Outlines Five Cloud Computing Trends – What They Really Mean. Retrieved April 27, 2012, from http://Cloudcomputing.sys-con.com/node/2259351

Basta, A. &. (2007). Computer Security and Penetration Testing (1st ed.). Alexandra: Delmar Cengage Learning.

Christodorescu, M. S. (2009). Cloud security is not (just) virtualization security: a short paper. In Christodorescu, In Proceedings of the 2009 ACM workshop on Cloud computing security (pp. pp. 97-102). Chicago: ACM.

Developerforce. (n.d.). Getting started with force.com. Retrieved March 26, 2012, from http://developer.force.com/gettingstarted

Eric, K., & Gelen, G. (2008, April 8). What Cloud computing really means. Retrieved March 26, 2012, from http://www.nytimes.com/idg/IDG_002570DE00740E180025742400363509.html

Go green, save greeen. (n.d.). The advantages of Cloud computing. Retrieved April 29, 2012, from http://www.simpleways2gogreen.info/the-advantages-of-Cloud-computing/

(2008). In B. Hayes, Communications of the ACM - Web science (p. p.11). New Yark.

Hinchcliffe, D. (2009, June 5). Eight ways that Cloud computing will change businesses. Retrieved April 29, 2012, from http://www.zdnet.com/blog/hinchcliffe/eight-ways-that-Cloud-computing-will-change-business/488

IBM. (2007, December). Cloud computing. Retrieved March 25, 2012, from http://searchCloudcomputing.techtarget.com/definition/Cloud-computing

Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2011). Cloud Computing Security Issues and Challenges. International Journal of Computer Networks.

Micheal, A., Armando, F., & Rean, G. (2010). A view of Cloud computing. Communications of ACM, 53, 1.

Miller, R. (2011, March 16). Understanding the Different Levels of Cloud Computing. Retrieved March 25, 2012, from http://www.businessservicemanagementhub.com/2011/03/16/understanding-the-different-levels-of-Cloud-computing/

Mogull, G. B. (2009, 1). Security guidance for critical areas of focus in Cloud computing v2. 1. Retrieved 6 10, 2012, from CSA (Cloud Security Alliance): http://www.Cloudsecurityalliance.org/guidance/csaguide. v2, 1, 2009.

Pardeep, K., Sehgal, K. V., & Singh, D. C. (2011). Effective Ways of Secure, Private and Trusted Cloud Computing. International Journal of Computer Science Issues,.

R. Buyya, C. Y. (2008). Market-oriented Cloud computing:Vision, hype, and reality for delivering it services as computing utilities. In In High Performance Computing and Communications (pp. pages 5–13). New York: IEEE.

WHSR. (2012, March 26). 15 Reasons to Fear Cloud Computing. Retrieved April 29, 2012, from http://www.webhostingsecretrevealed.com/featured-articles/15-reasons-to-fear-Cloud-computing/