ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (42-48), Month: January - March 2015, Available at: www.researchpublish.com

# Security Issues and Survivability of Cloud Computing In Nigeria

[1]D.W.S ALAUSA, [2]A.E DUROSINMI

[1]Department of Computer Engineering, Federal Polytechnic Ilaro, Ogun State. Nigeria
[2]Department of Computer Engineering, Moshood Abiola Polytechnic, Abeokuta, Ogun State. Nigeria

***Abstract:*** **The snag in the existing models of computing and how it slows down the rate of computing cannot be overemphasized. Thus the need for improvement and another approach/dimension into computing arises. Therefore, cloud computing an emerging trend in information technology which is an internet –based computing is used to provide potential cost reduction through optimized and efficient computing. Since it provides people the way to share distributed resources and services that belong to different organization. This paper identifies the main vulnerabilities in this kind of systems and important threats found relating to it and its environment as well as to identify and relate vulnerabilities and threats with possible solutions.**

***Keywords:*** **Cloud Computing, Cloud Services, Cloud security &Infrastructure.**

## 1. INTRODUCTION

Cloud computing (‘cloud’) is an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them.

Cloud enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing.

More specifically, cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down; providing for an on-demand utility-like model of allocation and consumption.

From an architectural perspective; there is much confusion surrounding how cloud is both similar to and different from existing models of computing; and how these similarities and differences impact the organizational, operational, and technological approaches to network and information security practices.

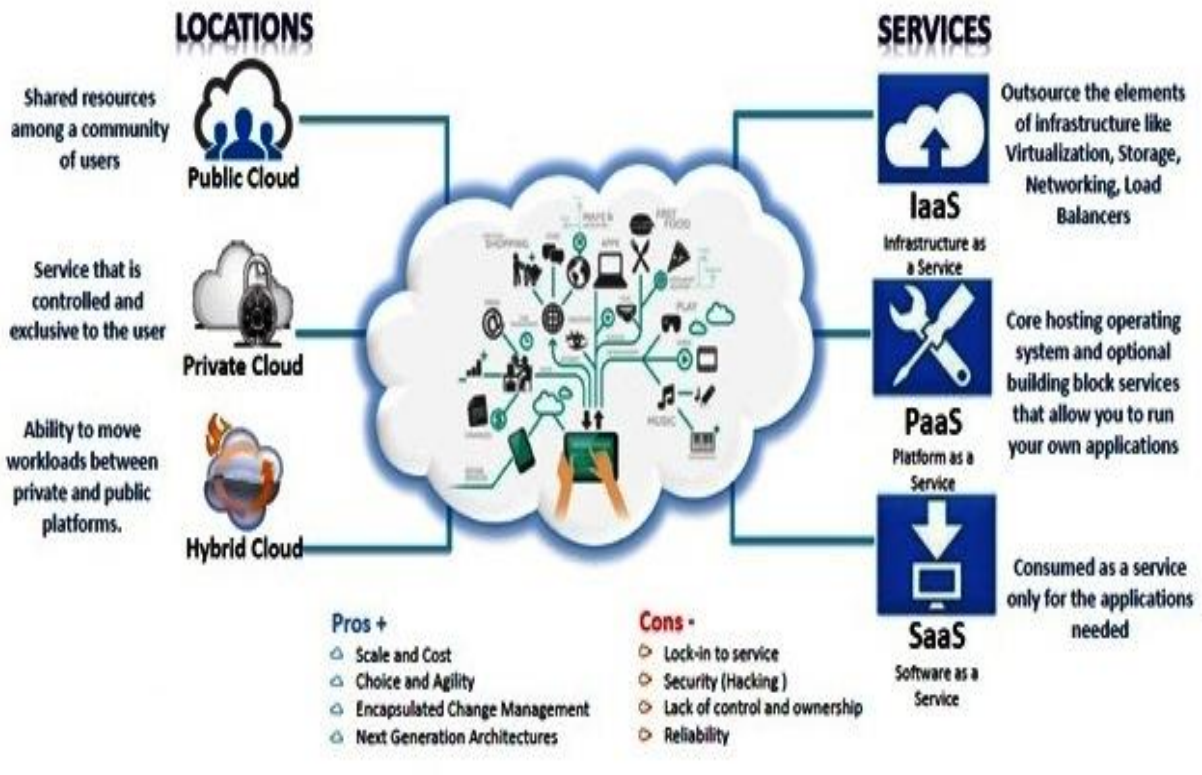
There are many definitions today which attempt to address cloud from the perspective of academicians, architects, engineers, developers, managers, and consumers. The keys to understanding how cloud architecture impacts security architecture are a common and concise lexicon, coupled with a consistent taxonomy of offerings by which cloud services and architecture can be deconstructed, mapped to a model of compensating security and operational controls, risk assessment and management frameworks, and in turn to compliance standards (Cloud Security Alliance, 2009) . All these resources can be accessed whenever necessary. In most cases the provider of the cloud sells his service as pay-per-use. This means that there is high flexibility in the use of these services as extra resources are always available (Strickland J., 2011)

The Cloud” is a term for various types of computing services which involve an internet connection. The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams. Cloud services are divided into three categories: Infrastructure-as-a-Service: Rented preconfigured servers, such as Amazon Web Services or Rack-Ssspace; Platform-as-a-Service: Rented computing systems and software to develop and host your own

programs; and Software-as-a-Service (SAAS): Rented applications or programs, such as Salesforce.com and Google Apps.

A distinguishing feature of "Cloud" services is that you select and pay for the service as needed. You don't have to maintain your own hardware or software. They are dynamically expanding, so you don't have to worry about capacity. A Cloud service can be offered to the public, or privately owned. The benefits are obvious: No more hardware or maintenance costs, buy only what you need, no upgrades to install, and access from anywhere. Costs can be lower, and are spread over time. There are some cautions: No internet connection means no service. You are entrusting your data to someone you will probably never meet. If they go out of business, or sell out, your data can vanish overnight. Data can be isolated – your Sales-force customer list won't connect to your QuickBooks online (yet). Upgrades or changes to the service can disrupt your business. Prices can change. Uptime guarantees don't always work out – not all vendors are reputable. The costs never end. You are already using "Cloud" services every time you use your email or browser. As internet connections become faster and more reliable, it matters less where your data or computing power is located. "Cloud" services have a lot to offer. Evaluate the offering carefully, paying attention to who owns your data, how it is backed up, and what happens if something breaks.

Often people do not know that they are using cloud computing. A simple example is Gmail or Google docs (http://docs.google.com/support/). It is a very good example as this is a free service and is explains perfectly what cloud computing is. Google doc makes it possible for you, and other users, to work online with a word processer with multiple users logged on. The complete document and service are stored online. Any changes made to a document appear real-time to the other users (Strickland J., 2011). Before diving into the growth of cloud computing, we should first understand the finer details of this technology. Everyone, in some shape or form, has heard of the cloud. Some see it as a buzz word, while others know it as a technology that can revolutionize the way we work; but few truly understand what the term 'Cloud Computing' really means. Simply stated, the cloud is any electronic data that is captured through the internet, but not stored on a device. It is the ability to perform computing tasks using software and applications that are not installed on your computer (or phone). While accurate, this definition is a little too simple (Daniel Tuitt, 2013). A deeper look at cloud reveals that it can be split-up into many different areas depending on the user's needs, as shown by the diagram below.




*(Retrieved from http://www.hcltech.com/blogs/transformation-through-technology/rise-cloud)*

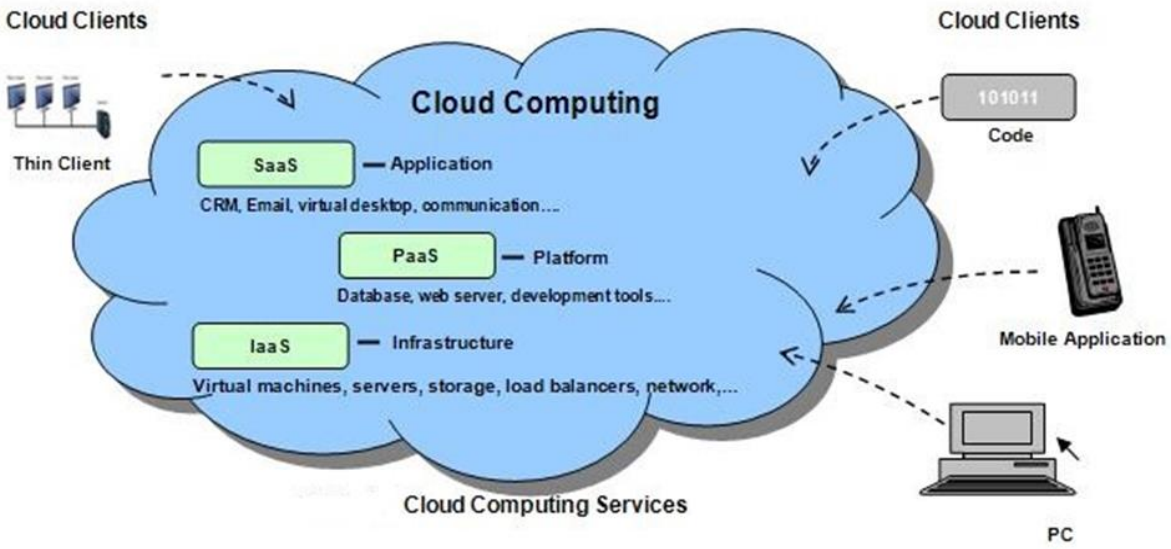
One of the main advantages of cloud computing is that it enables the user to increase storage capacity without the need to buy new hardware. In addition, it allows the use of different applications and provides access to music, TV programmes, and more on demand via the Internet. With all these different cloud products and services being offered, it can be difficult for any organization to understand it well enough to readily accept and implement cloud computing (Daniel Tuitt, 2013).

## 2. TYPES OF CLOUD

i. Infrastructure as a Service (IaaS) The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

ii. Platform as a Service (PaaS), The capability provided to the consumer is todeploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

iii. Software as a Service (SaaS), The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, oreven individual application capabilities, with the possible exception of limited user- specific application configuration settings (Cloud Security Alliance, 2009).




(*Retrieved from http://www.kingandwood.com/article.aspx?id=china-bulletin-2013-12-01&language=en)*

IaaS includes the entire infrastructure resource stack from the facilities to the hardware platforms that reside in them. It incorporates the capability to abstract resources (or not), as well as deliver physical and logical connectivity to those resources. Ultimately, IaaS provides a set of APIs which allow management and other forms of interaction with the infrastructure by consumers.

PaaS sits atop IaaS and adds an additional layer of integration with application development frameworks; middleware capabilities; and functions such as database, messaging, and queuing; which allow developers to build applications upon to the platform; and whose programming languages and tools are supported by the stack.

SaaS in turn is built upon the underlying IaaS and PaaS stacks; and provides a self-contained operating environment used to deliver the entire user experience including the content, its presentation, the application(s), and management capabilities.

It should therefore be clear that there are significant trade-offs to each model in terms of integrated features, complexity vs. openness (extensibility), and security. Trade-offs between the three cloud deployment models include:

•Generally, SaaS provides the most integrated functionality built directly into the offering, with the least consumer extensibility, and a relatively high level of integrated security (at least the provider bears a responsibility for security).

•PaaS is intended to enable developers to build their own applications on top of the platform. As a result it tends to be more extensible than SaaS, at the expense of customer- ready features. This tradeoff extends to security features and capabilities, where the built- in capabilities are less complete, but there is more flexibility to layer on additional security.

•IaaS provides few if any application-like features, but enormous extensibility. This generally means less integrated security capabilities and functionality beyond protecting the infrastructure itself. This model requires that operating systems, applications, and content be managed and secured by the cloud consumer.

In the case of SaaS, this means that service levels, security, governance, compliance, and liability expectations of the service and provider are contractually stipulated; managed to; and enforced. In the case of PaaS or IaaS it is the responsibility of the consumer's system administrators to effectively manage the same, with some offset expected by the provider for securing the underlying platform and infrastructure components to ensure basic service availability and security. It should be clear in either case that one can assign/transfer responsibility but not necessarily accountability (Cloud Security Alliance, 2009).

**2.1 Clouds Deployment Models:**

Regardless of the service model utilized (SaaS, PaaS, or IaaS) there are four deployment models for cloud services, with derivative variations that address specific requirements:

•**Public Cloud.** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

•**Private Cloud.** The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off- premises.

•**Community Cloud.** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may exist on-premises or off-premises.

•**Hybrid Cloud.** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

It is important to note that there are derivative cloud deployment models emerging due to the maturation of market offerings and customer demand. An example of such is virtual private clouds — a way of utilizing public cloud infrastructure in a private or semi-private manner and interconnecting these resources to the internal resources of a consumers' data centre, usually via virtual private network (VPN) connectivity.

**2.2 Cloud Computing And Its Constraints In Nigeria:**

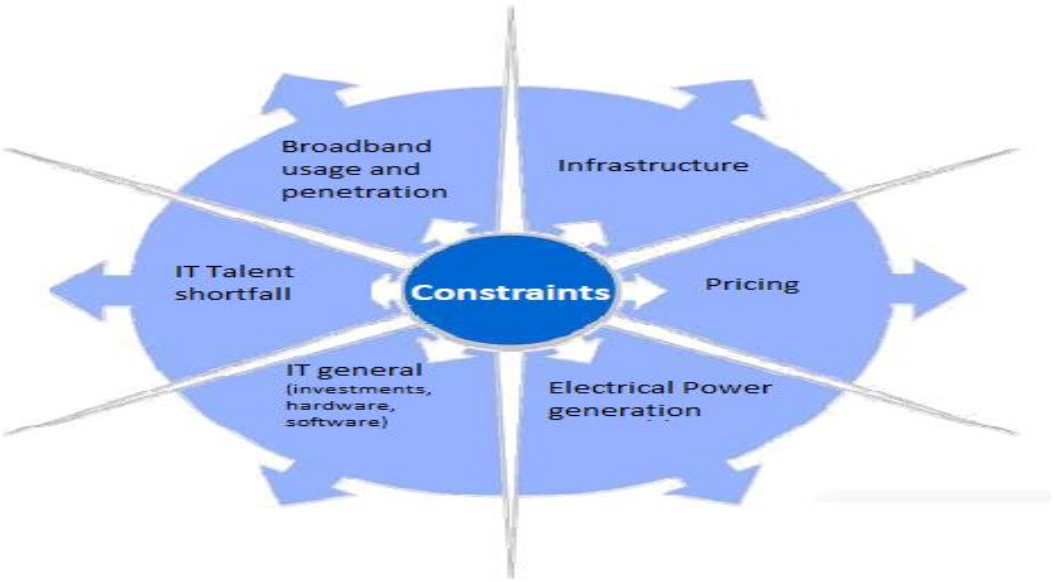
When someone brings up cloud computing, people either embrace it for its usability or ignore it due to a lack of understanding or concerns over its risks. As with any new form of technology, there will always be critics who first dismiss something that later becomes a game-changer. Just think of a world in which everyday technology such as Bluetooth, fibre optics or even the internet did not exist because a few close-minded individuals were unable to see the potential.

Many people are against transforming their business to a cloud based model due to the inherent risks involved, such as security issues, data being tampered with and data ownership once uploaded. In addition to the internal politics and operational barriers that many businesses face, making the transition to cloud based solutions can be an uphill battle. These fears are especially strong in industries that are governed by many regulations, and were heightened with the recent high profile viral attacks in which large online organizations had personal customer data stolen by hackers. It is no wonder that some organisations are nervous about adopting this technology (Daniel Tuitt, 2013).

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (42-48), Month: January - March 2015, Available at: www.researchpublish.com

Factors that generally affect information and communication technology in developing countries such as:

i. Broadband usage and penetration
ii. IT general(investments, hardware, software)
iii. Electrical power generation and consumption
iv. pricing
v. Government (ICT promotion)




## 3. MOTIVATING FACTORS AND CHALLENGES IN NIGERIA

1. Cloud computing is an inevitable evolution which is rapidly spreading in the marketplace.
2. Cloud computing is happening today because of the confluence of four factors: concept, suitability, technology and change in attitude.
3. Cloud computing can be broken into five distinct categories: Infrastructure, Platform, Software, Process and Orchestration.
4. Common roles are emerging in the cloud: Provider, Enabler, Broker, Store, Exchange and Assurance.
5. The benefits and risks of cloud computing are standard to the evolution of any activity.
6. Care should be taken with many of the assumptions behind the cloud, including: infinite supply, capability, commodity provision, heterogeneous demand, good-enough components and well-ordered markets.
7. Care should be taken in areas such as increased organizational strain, increased competition through reduced barriers to entry, the legacy question and choice of future standards.
8. Numerous strategies exist to balance the benefits and risks of cloud computing, including hybrid solutions, use of marketplaces and use of brokers.
9. Beware the misconceptions of cloud computing, including a reduction in overall IT expenditure, green cloud and virtual data centres as clouds.
10. Vendor strategies are not always obvious.
11. The overall consequences of the cloud include increased rates of innovation, disruption to existing vendors and potential loss of barriers to entry.
12. Loss of barriers to entry may also disrupt mechanisms of control.

13. The impact of cloud computing is not confined to companies.
14. The future of cloud computing is likely to be focused on Platform and Process.

## 4. COUNTER MEASURE TO MITIGATE RISKS

1. Risk management and (legal) compliance issues must be well defined in the contract between Cloud Computing provider and customer and should enable transparency with regard to the processing and Storage of data, e.g. the physical location of data storage. In this way the trust between the Cloud Computing provider and customer can be strengthened.
2. The service provided shall be compliant with the regulation and legislation that the customer needs to follow, and also customers should be enabled to be compliant with the respective regulation and legislation.
3. The communication line between the Cloud Computing provider and the customer has to be adequately protected to ensure confidentiality, integrity, authentication control and further to minimize the risk of denial-of-service attacks. An open and clear specification of the measurements taken to ensure the security of the communication line should be obligatory for any Cloud Computing provider and should be based on open and transparent standards and technologies.
4. The Cloud computing providers should be obliged to ensure data confidentiality.
5. Mandatory deletion of data should be included into potential regulation of Cloud Computing services, but it should not be relied upon too much.
6. The fact that there is no guaranteed complete deletion of data needs to be considered, when data are gathered and stored.
7. In order to guarantee the availability of data, local backup of essential data by customers should be considered.
8. Development and better promotion of software that enables local data transfers between devices should be encouraged.
9. The telecommunications network that supports the cloud computing services should be secured and protected against malware and DOS attacks.
10. Adequate logging and auditing should be provided. An external audit can be beneficial for the reputation of the Cloud Computing providers as well as for strengthening the trust with the customer.
11. Non-professionals (e.g. the usual user) should be educated with regard to the new paradigm. Education should prepare them to make competent decisions on using Cloud Computing services including what information should be transferred into the Cloud and under what circumstances.
12. Professionals should be skilled to manage the new types of risks.
13. Given that some regulation will be needed in the future, e.g. to balance the power between providers and customers of Cloud Computing services, it would be wise to consider its weaknesses and issues before Cloud Computing becomes a critical service or infrastructure. It needs to be checked which of the dimensions of conflict and regulatory potential will be relevant (e.g. the guarantee and liability with regard to confidentiality and integrity of processed data). In particular when a Cloud Computing provider becomes part of a critical information infrastructure some regulation or limitations concerning their possible takeover by another party may be appropriate.
14. Research on the basic concepts and issues in informatics, security, and privacy and their consequences And trade-offs with regard to Cloud Computing should be encouraged.

## 5. CONCLUSION

This paper, x-rayed a step forward to cloud computing, despite its critics and drawbacks it seems that Cloud Computing is here to stay. Present economic situation will force more and more organizations at least to consider adopting a cloud solution. We have considered the risks and benefits of cloud computing.

Future research will include a study regarding the level of acceptance and the implementation effects of Cloud Computing in Nigeria.

## REFERENCES

[1] A Lifecycle Approach to Cloud Computing (2011): Retrieved from http://www.lef.csc.com/publications/911

[2] A Security Analysis of Cloud Computing Retrieved from http://cloudcomputing.sys-con.com/node/1203943

[3] Cloud computing in Nigeria (2012): Retrieved from http://www.slideshare.net/c3dube/cloud-computing-nigeria

[4] Cloud Computing (2013): Key Telecommunication Regulatory Issues For Foreign Service Providers In China Retrieved from http://www.chinalawinsight.com/ 2013/11/ articles/ corporate/ cloud- computing- key-telecommunication-regulatory-issues-for-foreign-service-providers-in-china-2/

[5] Cloud Services (2013): Do Risks Outweigh Benefits Retrieved fromhttp://www.ipedr.com/vol22/6-ICEBM2011-M00013.pdf

[6] Cloud Security Alliance (2009): Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Retrieved from https://cloudsecurityalliance.org/csaguide.pdf

[7] Daniel Tuitt, (2013): Rise of the Cloud Retrieved fromhttp://www.hcltech.com/blogs/transformation-through-technology/rise-cloud

[8] Durosinmi, A. et al. (2014): Mitigating Cloud Computing Security Issues Through Contingency Planing. A proceeding of iSTEAMS Honours Conference 2014 International Conference on Working the Angles (29th -30th September, 2014). Auchi Polytechnic, Auchi, Edo State. Nigeria.

[9] Mell, P., Grance, T., (2009). The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. NIST special publication, 2011 National Institute of standards and technology. 145(6).

[10] Strickland, J. (2011): How cloud computing works. Howstuffworks.com. Retrieved from http://computer.howstuffworks.com/cloud-computing.htm

[11] The Future Of Cloud Computing Opportunities For European Cloud Computing Beyond 2010: Retrieved from http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

[12] What is "The Cloud"? Retrieved from http://www.toriangroup.com/Resources/ Articles By Topic /IT Management /What is TheCloud.aspx.