World Journal of Innovative Research (WJIR)
ISSN: 2454-8236, Volume-7, Issue-2, August 2019 Pages 49-51

Securing Cloud Platform for Enhanced Patronage

Adeniyi Akanni

***Abstract*— The technological world faces so rapid changes to bring the world a relief each day. The hitherto worries of managing a servers room, providing floor space, trained staff and other associated administrative overhead are lifted through cloud technology. Despite the huge potentials cloud computing generally offers, security concerns of data moved to Cloud are major reasons for organizations not to embrace this technology. This paper proposed a solution for securing the cloud platform.**

***Index Terms*— Cloud Computing, Cloud Service Provider (CSP), Infrastructure-as-a-Service (IaaS), Platform as a Service (Paas) and Software as a Servise (SaaS).**

I. INTRODUCTION

Cloud computing has provided a good support for organizations and business entities to leverage on. This is done by providing not just the expertise in the services rendered by the CSPs but by making the company to focus on their core functions. By so doing, the individual overhead cost is shifted to the CSP. Part of the cost includes: procuring servers from time to time (which keep arising due increased volume or obsolesce), office space to house, security apparatus (such as security guards, register and close circuit television) and expensive skilled labour (both in terms of hiring and keeping them). It should be noted that, Cloud computing is mutually beneficial to both CSP and outsourcing company. The former enjoys the economy of scale since it has the luxury of having so many organizations and the services would still be as if for one – the more, the merrier. However, proper definition of clients must be done to avoid mix ups.

II. PREVIOUS RELATED WORKS

Mell et al (2011) defined cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as network, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The benefits of cloud computing are enormous ranging from cost to expertise (Zimmermann, 2001; Brooks, 2010; Badger et al, 2010). It has observed that there is always a measure of difficulty in assessing the required bandwidth and hence, payment for the Internet Service Provider (ISP) especially in bandwidth intensive environment may be quite difficult to measure. However, John, (2013) explained that Cloud computing provides a leeway out this. A major derivable benefit from cloud computing is the ability for the cloud service customer to cede the responsibility of providing infrastructure to the CSP. Hence, banks need not bother about whether or not the bandwidth paid for is being sublet to other customers.

In essence, resources such as network, servers, space can be provisioned and released with minimal management effort or service provider interaction (Al Shehri, 2013). There are basically, five characteristics**,** three service models, and three deployment models in cloud computing. The service models are: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

The following are the main Deployment Models in cloud computing (fig 1):

A. Private cloud: this is a type of model deployed for the use of a single organization comprising multiple consumers

B. Public cloud: this is for the use of the general public. Ownership may be by individuals or business or government organization, or some combination of them.

C. Hybrid cloud: this is made up of two or more distinct cloud infrastructures (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).

D. Cloud computing, like other forms of virtualization, has some negative security implications (Wooley, 2011). According to Scarfone et al (2011), systems that involve of layers of technologies would have complicated security implications. Unless well attended to with reasonable assurance, it will always be a concern to business owners. Giacomo and Brunzel (2010) have however indicated that traditional outsourcing is similar to cloud computing. Thus, if security concerns can be addressed traditionally then they can in the cloud. A recent survey conducted by a consulting outfit, emphasized that despite the security reasons surrounding cloud computing more than 30% of the respondents agreed to move to cloud within the next 18 months (KPMG, 2013). The survey further disclosed that about 70% of the respondents believed that cloud computing is already delivering its benefits to the users. This goes further to say that Cloud computing is a way to go. Although there may be some security issues, they should be addressed to fully reap the potentials. Arnesen (2013) further corroborates this fact by explaining that he was not aware of any specific case of data compromise traceable to Cloud vendors. This is so because significant resources are being deployed to safeguard information assets placed in

Adeniyi Akanni, (Ph.D., CISA, CRISC, ITIL, ISO27001LA)
Anchor University Lagos, Nigeria

the cloud. It should therefore motivate more companies to consider migration to cloud.

III. BASIC NECESSITIES FOR SECURING CLOUD PLATFORMS

The following basic factors are necessary for securing cloud platform for clients (taking for granted that cost is not an issue since negotiation can be done on that:

A. Availability of IT Policy by boards of both parties. This is necessary to provide the framework.
B. Memorandum of Understanding where each party's roles and liability will be clearly spelt out and signed.
C. The CSP should also be certified by an appropriate authority.
D. The right to audit should be clearly communicated so that the client can be reassured of needed safeguards.
E. Robust access control to prevent unauthorized access.
F. Alternate site should be available for the CSP to provide seamless activities during routine maintenance or disruption.
G. Regular training of the client's staff is also necessary to ensure that no weak link exists in the chain.
H. Proper definition of clients must be maintained to ensure there are no mix up of data.

IV. METHOD EMPLOYED BY THE RESEARCHER

The researcher was in Nigeria whereas the CSP, Database Mart LLC was in USA. The choice of a CSP was based on financial consideration, a distant location as well as security of data. IaaS was adopted. In a way to demonstrate this, the researcher had a domain name by which he was identify and a password for authentication. Access to the database on its own was further controlled to minimize risk of compromise. From his base in Nigeria, the server was accessed remotely via the internet as if it was in the same building. The CSP provided the needed facility to check if it was on or not. This facilitated troubleshooting by pinging to see if the host is up already or not.

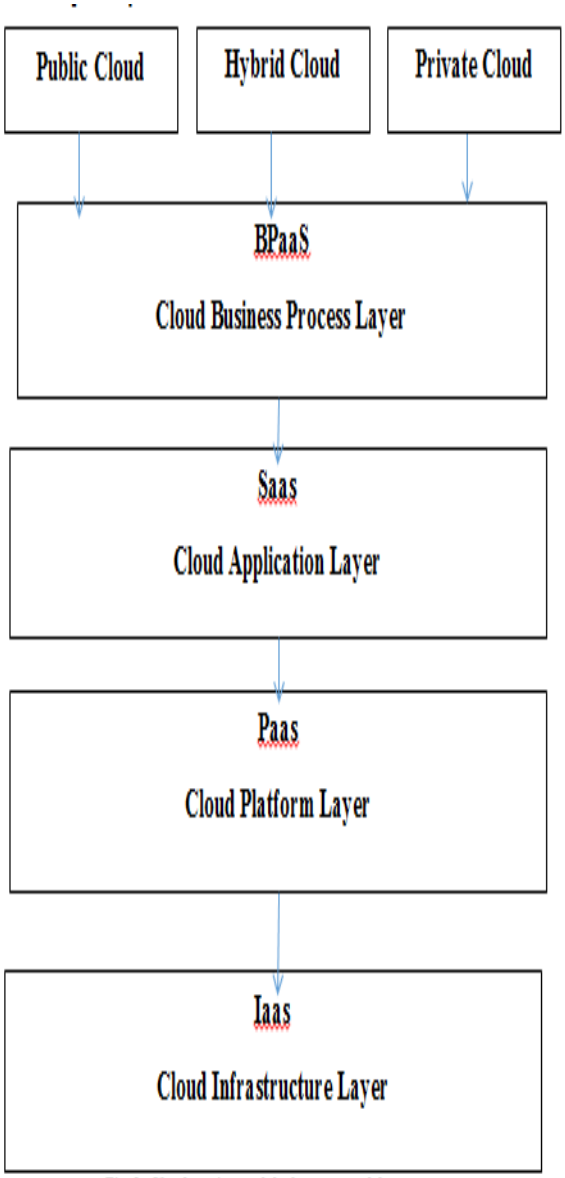

Fig. 1: Cloud services and deployment models

(Source: Al Shehri, 2013)

V. CONCLUSION

The researcher observed that distance was not a barrier to outsourcing. Despite the intercontinental distance, connection was seamless. Fear of data mix up or outright lost can be minimized. This was achieved by the researcher through strong access control. The fees charged by CSPs are not significantly different and can always be negotiated for better price. Thus, the work shows that organizations can embrace cloud computing for its numerous benefits having put into consideration necessary safeguards as contained in the work.

REFERENCES

[1] Al Shehri, W. (2013).Cloud database – database as a service. International Journal of Database Management Systems (IJDMS) Vol. 5, No. 2, April 2013.
[2] Badger, L., Bohn, R., Chandramouli, R., Grance, T., Karygiannis, T., Patt-Comer, R. and Voas, J. (2010).Cloud computing use cases.www.nist.gov.

[3] Brooks, C. (2010). How to build an application for the cloud.www.searchcloudcomputing.techtarget.com
[4] John, S. (2013). Efficient bandwidth drives cloud computing. www.Nigeriacommunicationsweek.comng.
[5] Mell, P. and Grance, T. (2011). The NIST definition of cloud computing. www.nist.gov.
[6] Zimmermann, R. (2011). Towards cloud computing. www.future-internet.com.