Survey of Cloud Computing Issues at Implementation Level

Omotunde A.A, 2 Awodele O, 3 Kuyoro S.O, 4 Ajaegbu C.
1,2,3,4 Department of Computer Science, Babcock University, Nigeria

ABSTRACT

Cloud computing is a new way of integrating a set of old technologies to implement a new paradigm that creates an avenue for users to have access to shared and configurable resources through internet on-demand. Cloud users are expected to increase exponentially in the future. In order to prepare for this stipulated increase, analyses of various factors have to be considered to ensure that cloud clients get the best out of the services offered by cloud providers. Amongst these factors, the ones that ensure successful implementation and adoption are of great importance to help cloud users make informed decisions that will have positive impact on their performance. Though, factors responsible for cloud computing success are inexhaustible, this paper presents some of the factors: ability to access and manage risk, performance, privacy, security, and financial issue.

Keywords: Cloud computing, deployment, performance, security, risk

1. INTRODUCTION

Cloud Computing is a new way of integrating a set of old technologies to implement a new paradigm that creates an avenue for users to have access to shared and configurable computing resources through internet on-demand (Burford, 2010). These resources which include networks, storage, servers, application and software can be provisioned quickly with ease and little management effort or interaction from the services providers.

This paradigm is gradually transforming how organizations purchase and manage computing resources. This in turn has changed the Information Technology model from having all the necessary hardware and software installed within the premises of the organization where they are needed to cloud providers who shoulder the responsibility of providing a range of IT activities including hardware and software installation, maintenance, backup and to a great extent provide security. This enables organizations to lower IT expenditure as well as operating and maintenance cost while redirecting their resources to core business activities thereby increasing productivity and competitive advantage.

Cloud services also include environments for application development and access to key technologies. Software and skilled IT personnel that could increase the overhead of an organization (Garrison et al, 2012)

From the definition of cloud computing, the following features can be identified:

- **Shared Infrastructure**: this characteristic of the cloud makes use of virtualized software model to share physical services, storage, and networking capabilities dynamically amongst many users according to demand (Mell & Grance, 2009). The user has no explicit knowledge of the physical location of the resources being used, except when the consumer requests to limit the physical location of his data to meet legal requirement.

- **Broad Network Access**: this characteristic enables users to access services over the network via standardized interfaces using not only complex devices such as personal computers, but also light weight devices such as PDAs and smart phones.

- **Rapid elasticity**: the available cloud computing resources are rapidly matched to the actual demand, quickly increasing the cloud capabilities for a service if the demand rises, and quickly releasing the capabilities when the need for drops. This automated process decreases the procurement time for new computing capabilities when the need is there, while preventing an abundance of unused computing power when the need has subsided (Kuyoro et al, 2012).

- **Connectivity**: All of the servers are connected to a high-speed network that allows data to flow to the Internet as well as between computing and storage elements.

Despite the numerous advantages that are provided by cloud computing services some factors are still militating against organizations in the adoption of cloud services. These factors include: uncoordinated adoption by stakeholders, inadequate business acumen, and various issues at the design and implementation levels. Because it is possible to waste resources in IT investment or have IT resources implemented in a non-optimized manner, organizations are unlikely to come to full realization of the benefits when cloud computing services fall short of expectations.

In light of the aforesaid, (Roseblum, 2012) opined that it is important to realize that like any other new technology there are some risks of failure. Due to these risks, 90% of Cloud Computing projects do not meet schedule, budget and the desired quality; 9% of large, 17% of medium, and 28% of small company projects were completed on time, within budget, and delivered measurable business and stakeholder benefits. Also, (Pradip, 2012) posited that one of the major reason why Cloud Computing project fail is because prospective
cloud users do not completely understand the financial realities of implementing it.

Thus, the aim of this paper is to identify and elucidate factors that ensure successful implementation and adoption of cloud computing services. Section 2 discusses service delivery and service deployment models in cloud computing. Section 3 discusses factors that guarantee successful implementation of cloud computing and section 4 gives the conclusion.

2. SERVICE DELIVERY AND DEPLOYMENT MODELS

2.1 Service Delivery Model

Cloud Computing has three distinct delivery models. They are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Figure 1 illustrates these models.

- **IaaS**: this is the foundation of all cloud services in which cloud vendors provide the basic infrastructure which includes (virtual) platforms, raw storage, firewalls and networking among many other. Applications are placed on these infrastructures thereby drastically reducing huge initial investment (monetary and otherwise) that business organizations encounter this focusing more on activities that will foster productivity. When implementing IaaS, hardware is completely abstract and customers consume infrastructure as a service having no need to bother about the underlying complexities.

- **PaaS**: the service delivery model sits directly above IaaS on the stack. At this level, cloud vendors abstract everything up to Operating System and middleware. This simply means that they (vendors) provide software and tools for building application to customer. It offers developers a service that provides a complete software development to testing and maintenance.

- **SaaS**: software is made available to cloud users over a network, in most cases, the internet on a pay-as-you go basis and it is usually accessed using a thin client via a web browser. SaaS is most often implemented to provide business software functionality to enterprise customers at a low cost while allowing those customers to obtain the same benefits of commercially licensed, internally operated software without the associated complexity of installation, management, support, licensing, and high initial cost (Kuyoro et al, 2011).

2.2 Service Deployment Model

The various deployment methods by which cloud computing can be implemented is in figure 2

- **Private Cloud**: Scalable resources are assembled together and hosted internally or externally and managed either by the organization internally or a third party to meet the need of a single organization for the sole purpose of operating in a more secured way as it is the most secured deployment model.

- **Public Cloud**: This is the most universal of all the models. Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis (Kuyoro et al, 2011).

- **Community Cloud**: This model is deployed for several organizations that have a common theme. This can also be managed internally or by third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more costly than a private cloud), so only some of the cost savings potential of cloud computing are realized.

- **Hybrid Cloud**: This is composed of a private cloud linked together with two or more clouds (public or community). Each of these clouds remain distinctive entities but are bound together thereby presenting the benefits of multiple deployment models. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets -for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter (Kuyoro et al, 2011).

3. FACTORS RESPONSIBLE FOR SUCCESS IN CLOUD COMPUTING

In spite of the fact that cloud computing offers numerous advantages, there still are some issues that hold back some efforts. These include: ability to access and manage risks, performance, security and privacy of data, trust and financial issue.

3.1 Ability to Assess and Manage Risk

(Heiser & Nicololet, 2008) posited that for an organization to be successful at using an external service (PaaS, IaaS, SaaS), proper risk assessment must be carried out to identify the security risks, privacy and compliance risks. The following should be evaluated when carrying out the assessment: privileged user access, compliance, location of data, data segregation, and recovery. However, for all these factors to be assessed, cloud providers must play an important role in making their operations as transparent to the customers as possible without disclosing sensitive information especially in situations where multi-tenancy of resources takes place. Cloud providers are able to win customer’s confidence by being as transparent as possible which in turn makes the customers aware of information about how their data will...
be protected so as to enhance the quality of their decision. Transparency in this context means apposite revelation of the governance aspects of security design, policies and practice.

3.2 Performance

Poor performance and non-availability of data to an end user means the same as the services required are not usable. (Blaisdell, 2012) highlighted some factors responsible for poor performance in cloud computing environment. These include: limited bandwidth, disk space, memory CPU cycles, Network connection and most importantly latency which reduces the end-to-end response time. This according to (Linthicum, 2012) happens because latency which is universal to cloud-based system is not taken into account by those who hold out cloud based applications. Most companies chose to adopt a federated cloud computing system, where some applications were located on public cloud, some applications on private cloud, and some legacy applications were accessible over VPN.

The only reasonable way to handle this volume of information is to have a performance management system that monitors the activity of all applications. However, most performance management systems monitor discrete values such as CPU usage and memory usage. These by themselves do not appropriately reflect response time as the end users experience. In light of this, (Linthicum, 2012) suggest that architecture and planning should be focused on, having at the back of their minds that services that are delivered are given to stretched out, slackly coupled systems where data, application, machine, and human that may reside thousands of miles away. Therefore, the use of buffers or a cache may help improve the architecture that deals with latency.
3.3 Security

There is no doubt that security has been the major barrier in the adoption of the cloud by organizations as the thought of running your software and storing sensitive data on someone else’s hard disk is rather frightening.

According to a 2009 IDC Survey, security was rated as the greatest factor for holding back organizations from implementing it. See figure 3.

Fig 3: IDC Survey rating the challenges of cloud computing

However, there are conflicting opinions concerning which party takes responsibility for security of data in cloud. At this point, it is needed to restate that the ultimate aim of implementing cloud computing is to benefit from economies of scale through the use of versatile resources, specialization, and other adeptness, thus reducing overhead cost. This however does not imply that responsibility for privacy and security should be reduced (Chandrareddy et al, 2012). In view of the aforementioned, (Megalhaes, 2012) posited that the responsibility for security and privacy of data lies with the data owner. He further considered it ‘reckless’ for cloud service users to totally depend on the service providers to secure and protect their data.

(Hamlen et al, 2010) opined that numerous security issues are associated with cloud computing, some of which lie with the service provider and most with the cloud service users because it encompasses various technologies which include networks, databases, operating systems, virtualization, resources scheduling amongst many others. In light of this, (Kuyoro et al, 2012) held forth that is expedient for organizations to apply security measures that will cater for the delivery method they adopt since threats differ from layer to layer. Organizations implementing Saas are to consider the security and integrity of their data as well authentication and authorization of their users. Those implementing PaaS get an integrated set of development environment that a developer can tap into without having a clue of what is going on underneath.

At this level, protection of data is also needed before sending any private information to the cloud (Kuyoro et al, 2012). Therefore, encryption of data while in transit and while stored on a third party platform and awareness of the regulation issues that may apply to data availability in different geographies is another issue that must be duly considered. The following are suggested by various authors to confront the issue of security at implementation level: Implementation of IPSec from the user’s end and Transparency of cloud providers. Transparency as a means of security may also be implemented. This simply implies that there is appropriate disclosure of the governance aspect of the security design, policies, and practices.

3.4 Trust

Though the responsibility for securing and ensuring privacy of data lies with the data owner (Megalhaes, 2012); they must relinquish direct control over some aspects of security. This includes the storage of data on the server of another organization amongst others. This situation of relinquishing control is rather inevitable because the whole idea of buying into cloud computing in order to reduce the cost of purchasing hardware will be forfeited if the hardware is eventually purchased in order to be in total control of their data.
In this situation, it is the duty of the cloud computing user to encrypt sensitive data before sending it out to another organization for storage. Also, both the cloud service provider and cloud customers must come to a consensus on data that will be handled. Cloud providers must assure their customers that their data will be properly protected. Non-disclosure agreements and heavily negotiated contracts amongst many other may be deployed as a legal document that indicates trust. This implies that appropriate disclosure of the governance aspects of security design, policies which explicitly explains the approach to security and illustrates an organization’s management position on security and risk will be given to customers to help build their trust in the vendors.

3.5 Financial

One of the advantages of cloud computing as posited by (Kuyoro et al, 2012) is that cloud computing enables the measuring of used resources as is the case in utility computing which can be used to provide resources efficiency information to the cloud provider and can be used to provide the consumer a payment model based in “pay-per-use”. The general perception of cloud computing cost is that it follows a price quantity model. However, some of the cloud pricing structures which include Microsoft’s online collaboration offering (dedicated vs. multi-tenant, volume discounts, existing Enterprise Agreement discounts and end of year discounts and Amazon’s Elastic Compute (EC2) offering (On demand, Reserved or spot instance pricing) make it difficult to ascertain how much will be paid by cloud users. In light of this, (Langley-Hawthorne, 2010) suggested that detailed financial models should be developed to give an accurate comparison of Cloud pricing vs. traditional approaches and what really happens when expected volumes change.

Also, Companies can save the considerable costs associated with building, maintaining, and operating a data center, especially power and cooling related expenditures. Additionally, the model allows firms to lower expenditures on support staff, particularly those providing infrastructure support, systems management, and help desk services. However, the cost of transferring data to and from public cloud and/or community cloud is likely to increase. Also the cost of computing resources is likely to be higher. (Dillon et al, 2010) opined that this is more common where the organization's data is distributed amongst a number of public/private (in-house IT infrastructure)/community clouds.

Therefore it is pertinent for cloud computing users to strike a balance amongst integration, communication, and computation. “Putting the computation near the data” as opined by (Gray, 2008) still holds so as to cut down the cost of communication.

4. CONCLUSION

Bearing in mind that cloud computing users are expected to grow exponentially in the coming years, this paper deliberated on the factors that cloud computing vendors and users must consider in having a successful cloud computing environment. It is believed that this study will help vendors and customers make the right choices when implementing various services in the cloud.

REFERENCES


AUTHOR PROFILES

Omotunde A. A. received M.Sc. in Computer Science from Babcock University in 2012. He is also a research student of Babcock University Postgraduate School, Nigeria. Currently, he is an Assistant Lecturer at Computer Science Department, Babcock University.

Awodele O. is a Senior Lecturer at Computer Science Department, Babcock University, Nigeria.

Kuyoro S. O. received M.Sc degree in Computer Science at the University of Ibadan, Nigeria in 2010. She is currently a research student of Babcock University Postgraduate School, Nigeria and an Assistant Lecturer at the Computer Science Department, Babcock University, Nigeria.

Ajaegbu C. received M.Sc. in Computer Science from Babcock University in 2012. He is also a research student of Babcock University Postgraduate School, Nigeria. Currently, he is an Assistant Lecturer at Computer Science Department, Babcock University.