Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

The Cloud Adoption Dilemma for Developing Countries: Key Challenges and Directions

Gilbert Barasa Mugeni
Ph.D- Information Technology
Communications Authority of Kenya, Nairobi, Kenya

Abstract: ***The Cloud promises to deliver a range of benefits including a shift from capital-intensive tooperational cost models, greater agility and reduced complexity. It can alsobe used to shift the focus of ICT resources to higher value-added activities for the enterprise, support business innovation and, potentially lower operational risks. However, it has been argued that as with any new technology offering, Cloud computing has certain degree of risks, and thatthese prospective benefits need to be examined carefully and mapped against a number of challenges including security, transparency, availability, performance, the potential for vendor lock-in, licensing constraints and integration needs. Other arguments have been advanced that over time, Cloud computing will not always save money. These issues, among others create a complex environment in which to evaluate individual Cloud offerings. As developing countries are confronted with the decision of adopting Cloud services, it is necessary that decision makers have sufficient knowledge on the subject for informed decision making. This paper aims, in the context of developing countries, to review the terms, characteristics, and services associated with Cloud computing, the arising technological, operational, and policy challenges, and suggest possible mitigation measures, with focus on the Cloud readiness and maturity assessment.***

Key words: Cloud adoption; Cloud readiness assessment; Cloud maturity, Developing countries

I. INTRODUCTION

Cloud computing is generally thought of as a model in which an external service provider delivers IT capabilities as a service to individuals or businesses [1], and has been taunted as being key in making affordable investment and use of ICTs by allowing for the sharing and scalable deployment of infrastructure, services, and applications as needed, from almost any location, and for which the customer can be billed based on actual usage [2].

Because of the evolving nature ofCloud technology, it is often difficult to have a standard definition of Cloud computing [2]. The US Department of Commerce's National Institute of Standards and Technology defines Cloud computing as"a model for enabling ubiquitous, convenient, on-demand network access to ashared pool of configurable computing resources (e.g., networks, servers, storage,applications, and services) that can be rapidly provisioned and released with minimalmanagement effort or service provider interaction" [3].

II. KEY CHARACTERISTICS

The key characteristics associated withCloud computing asidentified by [3] are:-

Shared Infrastructure:-Enables the sharing of physical services, storage, and networking capabilitiesacross a number of users.

Dynamic Provisioning:-Allows for the provision of services based on demand requirements thus enabling the expansion and contraction of service capability, as needed.

Network Access:-Enables network access to services and applications from a broad range of devices such as PCs, laptops, and other portable and mobile devices.

Managed Metering:-Consumers are billed for services according to how much they have actually used during the billing period.

III. SERVICE MODELS

The three main Cloud computing service models are identified by [4] areas follows:

Software/applications as a Service (SaaS):-Consumers access and use an applicationor service that is hosted in the Cloud. An example of this is Microsoft® Office 365 available as a Cloud-based service.

Platform as a Service (PaaS):-Consumers access platforms in the Cloud, enabling them to deploy their own software and applications.The operating systems and network access are not managed by the consumer, but by the service provider.

Infrastructure as a Service (IaaS):-Consumers manage systems stored in the Cloudi.eoperating systems, applications, storage, and network connectivity, but do not themselves control the Cloud infrastructure.

In addition to these, [4] [5] identify emerging Cloud platforms such as, **Business Processes as a Service (BPaaS), Communications as a Service (CaaS)**, and **Security as a Service**.

IV. DEPLOYMENT MODELS

According to [6], Cloud services can be used in a private, public, or hybrid setting. Below is a brief description of each model.

Private Cloud:- The Cloud infrastructure is deployed, maintained and operated for a specific organization. The operation may be in-house or with a third party on the premises. Privately-hosted Cloud services are generallyconsidered a safer but more costly option than Cloudservices using a shared or public arrangement [6].

Public Cloud:-The Cloud service is available to the organization on a commercial public basis by a Cloud service provider. This enables a consumer organization todevelop and deploy a service in the Cloud with minimal financial costs compared to the capital expenditure requirements normally associated with other deployment options [6][7].

Hybrid Cloud:-The Cloud service is a combination of a number of Clouds of privateor public nature, with the ability to allow data and applications movement among the Clouds [6][7].

Other authors identify a fourth model, the **Community Cloud**, which is essentially a variant of the private Cloud. For example, [3] defines a Community Cloud as an arrangement where a number of organizations with similar objectives and requirements share the Cloud infrastructure. In this case, the capital expenditure costs for establishment as well as operational costs are shared among the organizations. As with the private Cloud, the operation may be in-house or with a third party on the premises.

The service, deployment, and the location variations in Cloudsare summarized by [8] ina Cloud computing dimensions schematic shown in Figure. 1 below:

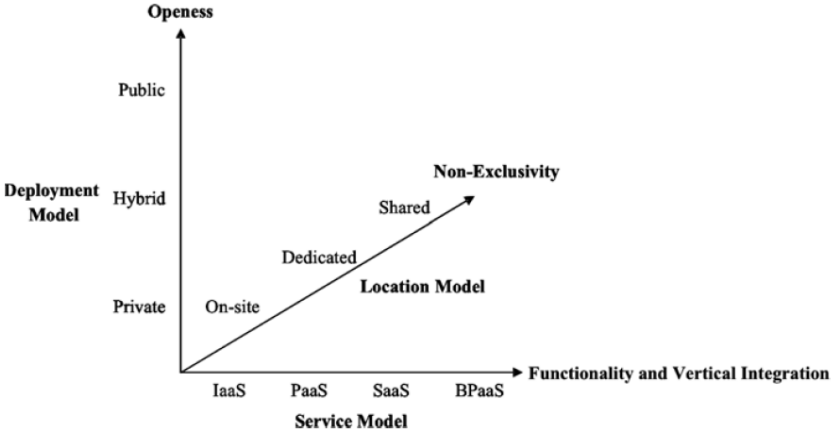

Fig. 1 : Dimensions of Cloud computing Source: Claudia et. al., (2011)

V. DRIVERS OF CLOUD COMPUTING ADOPTION

There are many drivers for the adoption of Cloud computing, the main ones being convenience, cost, speed, scalability, and redundancy among others.

Convenience:-It's often easier, cheaper and quickerto deploy a SaaS application than investing in an in-house enterprise software [4]. The Cloud also allows for rapid provisioning and use of services by the clients [6].Furthermore, the deployed application can be available from anywhere.

Cost:- Cloud computing and especially IaaS models lead to reduction in both the capital and running costs of hardware, software, and associated licenses [4][5]. In the case of data centres, the associated rental, power consumption and cooling costs are significantly reduced [4].

Speed:-Projects involving Cloud computing may often be deployed with faster speedcompared to conventional projects [4].

Scalability:-Cloud computing provides a scalable online environment thus enabling growth and re-sizing in accordance with the user's requirements. This is specifically important for small and medium enterprises (SMEs) that may not have sufficient technological, financial and human resources to invest in ICT infrastructure [4][6].

Redundancy and Business Continuity:-External hosting of applications and storage ensures redundancy and business continuity in the event of failure. Service Level Agreements (SLAs) with competent service providersfurther ensure availability [5][6].

Other researchers [2][4][8] have identified a number of other salient benefits of Cloud computing including efficient processes, enhanced security, legacy modernization, and central administration of policies.

VI. CHALLENGES OF CLOUD ADOPTION

The challenges to Cloud adoption can be sub-divided into technological, policy, and operational challenges [7], with the biggest challenge being Cloud security [9].

Operational Challenges:-These encompass costs, governance, management and skills related challenges that would hamper effective Cloud adoption within an organization [8][9]. With large investments already made in theon-premise infrastructure or data centers, the cost to move workloads to Clouds, both in terms of human expertise and management toolscan be quite an undertaking. Skills related challenges encompass the service provider, the system support staff, and users. According to [10], operational challenges can be effectively overcome by appropriate planning for the Cloud migration. Ideally, small batches of functionality should be gradually moved to the Cloudin a phased fashion.

Policy Challenges:-Policy challenges revolve around storing sensitive and proprietary data on external environment and the associated risks, and involve institutional, national or even policies of third parties on Cloud computing, where Cloud services are sought from foreign service providers [10]. Appropriate data protection actsand policies as well as intellectual property rights are key in resolving these challenges [11]. A key challenge is in the processing of personal data. Researchers have suggested a new approach, "Privacy by design" to mitigate this, and consists of building in of privacy requirements from the very outset of a system's development and throughout its life cycle [12].

Technological Challenges:-Technological challenges range from connectivity problems in terms of bandwidth availability to security concerns [11].According to a Forbes report on the top most brutal cyber attacks of the year of 2014, Sony, Target, E-Bay and Home Depot suffered major cyberattacks, among others. Many of these attacks were eventually associated with Cloudpresence of the hacked entities. Security concerns in Cloud computing revolve around Confidentiality, Integrity, and Availability (often referred to as the "CIA triad" [13], i.e that information is accessed only by authorized persons, is reliable, and available whenever needed. In particular, researchers [11][12] have recently raised concerns with Cloud services providers with regard to 5 key security areas namely:

(i). **Shared Access**:- Due to the multi-tenancy nature of the Cloud, a flaw could allow other tenants or attackers to see all other data or to assume the identity of other clients [11].

(ii). Virtual Exploits:-Cloud computing technology heavily relies on the ability of multiple virtual machines (VMs) to concurrently run different software applications on different operating system environments on a single physical machine [6]. Recent research shows that the shared technology inside the Cloud computing environments is susceptible to attacks [9]. For example, by identifying the target VMs on a Cloud computing servers, attackers can potentially steal data hosted on the same physical machine [9].

(iii). Access Control: - Access Control includesAuthentication, Authorization, and Data Protection [10]. There is a possibility of sharing a common namespace with the vendor or indirectly with other tenants. Private keys for data encryption could also be shared [11] thus compromising Access controls.

(iv).Availability:-Redundancy and fault tolerance are under the control of the service provider [11]. Cloud services still go down despite fault tolerance measures taken. Sometimes customer data may be lost either due to the Cloud provider fault or due to a malicious attack [12].

(v). Data Ownership:-This is the big question of whose data is the data on the Cloud?. Cases are known where Cloud providers have clauses in their contracts that explicitly give them rights to the data stored by them [12]. This would give them protection in case of legal mitigation.

Possible methods to mitigate these threats include focusing on both technical and legal measures to address potential security problems [12]. The former include encryption and use of trusted platform modules, while the latter is based on legal arrangements with service providers [13]. However, the bottom line is that Cloud visibility is still low, i.eeven when the Cloud computing risks are known, they're difficult to quantify with accuracy [14].

VII. CLOUD READINESS ASSESSMENT

According to [15], Cloud readiness assessment involves a critical review of an organisation's technology, processes, and people, and offers a number of insights into:

(i). The readiness of an organization in the technology, processes, and people domains.

(ii). Change management, process analysis, and application rationalization.

(iii). Governance and executive support.

(iv). Vendor selection and proof of concept.

Addressing the necessity of Cloud readiness assessment, [16] singles out eight key areas of assessment namely, Business Strategy, Organization, Governance, Projects & Services, Architecture, Infrastructure, Information, and Operations. These areas are further classified into two broad domains namely, Technological and Organizational dominated [16], Figure 2.

Accordingly, [16] describes these domains as follows:

Business Strategy:- High level considerations that motivate the Cloud initiative, i.e Business motivation, expected benefits, costs etc.

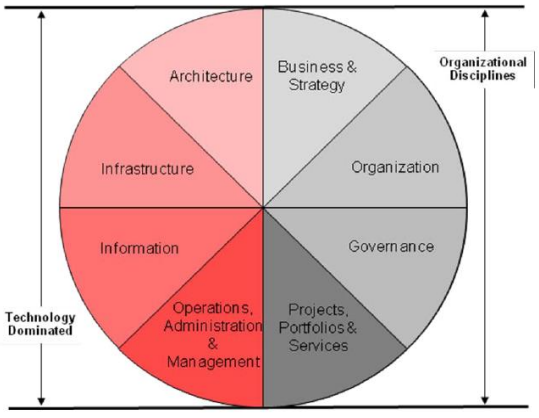

Fig. 2. Oracle's Cloud maturity model domains Source: Oracle, (2011)

Architecture:-Defines the overall architecture and guidelines for various stakeholders engagement.

Infrastructure:-Service infrastructure and the tools that provide the technical foundations.

Information:-Cloud information such as metadata management and customer entitlement.

Projects & Services: -Planning and building of Cloud services, including portfolio information.

Operations & Management:-Details of the post deployment aspects of operations, administration, and management.

Organization:-Organizational and skills competence around Cloud computing.

Governance:-Governance structures related to institutional policy, risk management and audit.

In related research, [8] identifies seven overall criteria to assess the Cloud readiness of an IT service namely Core Business, Importance/Availability, Standardization, Degree of Distribution, Network Connectivity, Identity Management, and Compliance. These criteria are further elaborated as below [8].

(i).Core Business relevance& differentiation- Is the IT service relevance high to the business and significantly contributes to turn over? Is IT service contribution to competitive position (differentiation) high?. If the relevance is low, and contribution low, the IT service is likely to be Cloudy ready.

(ii). Importance/Availability- Is the IT service critical and availability high? If the IT service is critical and availability is high, the IT service is likely to be Cloudy ready.

(iii). Standardization- Is the IT service life cycle complex (highly integrated and interdependent with other systems)?. Are IT services adopted to organizational needs (non-standardized)?. If the IT service has a non-complex life cycle and is standardized, the IT service is likely to be Cloudy ready.

(iv). Degree of Distribution-If IT service administrative offices are distributed over large geographic regions or globally, the IT service is likely to be Cloudy ready.

(v). Network Connectivity-An IT service with low bandwidth requirements and low latency is likely to be Cloud ready.

(vi). Identity Management-An IT service has low integration if it has it's own identity management independent of the enterprise's identity management. The IT service administration is centralized if the provisioning of users follows central guidelines including conventions for naming and security. A weakly integrated IT service with a centrally administered identity management is likely to be Cloud ready.

(vii). Compliance- Realization efforts are high if extensive organizational and technical provisioning is to be fulfilled; Requirements are high if the processed data need to match strict legal and regulatory standards including organizational specific standards. An IT service with low realization and weak compliance requirements is likely to be Cloud ready.

VIII. CLOUD MATURITY

The concept of Cloud maturity, is modelled on the principles of the Capability Maturity Model (CMM), and it's succeesor, the Capability Maturity Model Integration (CMMI)[16][17], both widely used in the software development industry[8][17].

Accordingly, [16] classifies the Cloud Maturity Model into six defined maturity levels progressing from "None" to "Optimised" as follows:-

None: - No Cloud approach is being taken or implemented.

Ad Hoc:-Cloud computing awareness is established, some elements of Cloud computing are beginning to be implemented, but with no cohesive Cloud plan.

Opportunistic:-An approach has been decided on, but has not been widely accepted, and redundant or overlapping approaches exist.

Systematic:- The approach has been reviewed and accepted. The documented approach is always or nearly consistently followed.

Managed:-The Cloudcapability is being measured and quantified via an approved governance structure. Appropriate metrics are gathered and reported.

Optimised:-Metrics are gathered, reviewed, and used to improve the Cloudcapability, with the potential to leverage inter-Cloud operations established. Assets are proactively maintained.

In another approach to Cloud maturity, [15] proposes a four stage model comprising Thinking, Initiating, Creating, and Riding the Cloud with the following key characteristics for each stage [15].

Thinking (About the Cloud):- Characterised by decentralised IT and lack of Standards and Policies. This is the initial stage of up to one year during which the major milestone should be to carry out executive and organisational awareness.

Initiating (Reach for the Cloud):-Spanning a period of 1-3 years, this stage is characterised by executive support, bussiness case and budget formulation, re-defined IT governance, hardware and software standards creation, and legacy mapping. The key milestones at this stage include the development of the governance structure, hardware and software standards, RFP and tendering process, and the proof of concept.

Creating (Organisational Cloud):-This stage is a period of 2-3 years with the major milestones including process analysis and improvement initiatives, change management, identification of technologies and vendor selection, SLA definition, rationalised and modernised IT landscape, and characterised by virtual desktop and infrastracture as a service (Iaas).

Riding (the Cloud):-This stage is characterised by functional and effective change management, Cloud adoption champions, centres of excellence for bussiness process improvement, co-existence of legacy and Cloud environments and applications available on the Cloud as a service. The stage depicts a fully functional Cloud development environment and may take a period of 2-3 years.

IX. CONCLUSION

Whereas the results of the Cloud readiness assesment will differ from one organisation to the other, [8] [15][16][17] variously identify a number of IT services as being Cloud candidate or "likely Cloud ready" namely, Intranet, Internet, Messaging, Internet Mail Gateway, Managed Server, Managed Work Station, Virus Protection, Patch Management, Vulnerability Management, IT service Manager Tool, Office and File viewer, Internet Access Gateway, Archiving, IT Help desk, and On-line collaboration among others. However, the exact number and ordering is dependendant on the specific readiness assessment results.

Finally, it should be noted that although presently in the Cloud arena, the emphasis is on educating clients on the Cloudtechnology and its benefits,this may soon be a thing of the past, as the main challenge for organisations will be how to get to the Cloud and stay there securely. As for now, as organisations dive into the future and join the Cloud bandwagon, some are also deep rootedin the previous legacy applications, some of them business critical thus slowing down adoption. The future will reveal whether the current critical Cloudreadiness assessments will remain dominant or whether procuring Cloud services will be as normal as we currently treat procuring common services such as energy.

This paper has attempted to provide a critical review of the terms, characteristics, and services associated with Cloud computing, the arising technological, operational, and policy challenges, and finally suggested possible mitigation measures, focusing on Cloud readiness and maturity assessment.

REFERENCES

[1] Desisto,R.P., Plummer, D.C.& Smith D.M., (2008).Tutorial for understanding the relationship between Cloud computing and SaaS. Stamford, CT: Gartner

[2] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. &Zaharia, M., (2010).*A View of Cloud Computing, Communications of the ACM, 53, 4, 50-58.*

[3] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J.&Brandic, I., (2009).Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility, *FutureGeneration Computer Systems, 25, 6, 599-616.*

[4] Rufat, F. T., & Zafar, J., (2014).*The use of Cloud technology in Corporate Information Systems.International Journal of Computers & Technology, Vol. 14, No. 1,ISSN 2277-3061*

[5] International Telecommunications Union -ITU, (March, 2012). *Privacy in Cloud Computing-ITU-T Technology Watch Report*

[6] Choo, K. R.,(October, 2010). Cloud computing: Challenges and Future Directions- Trends and Issues in Crime & Criminal Justice, Australian Institute of Criminology, Australian Government

[7] Cloud Security Alliance,(2009). Security guidance for critical areas of focus in Cloud computing V2.1.*http://www.Cloudsecurityalliance.org/csaguide.pdf*

[8] Claudia, L., Thomas, B., &Ullrich,T.,(2011). Assessing Cloud Readiness- Introducing the Magic Matrices used by Continental AG available at: http://www.mtm.uni-koeln.de/team-loebbecke-publications-conf-proceedings/Conf-154-2011-AssessingCloudReadiness.pdf

[9] Hardesty,L.,(2009). *Secure computers aren't so secure. MIT press release 30 October. http:// www.physorg.com/news176107396.html*

[10] Kaufman, L.M.,(2009). Data security in the world of Cloud computing. *IEEE Security & Privacy July/August: 61–64*

[11] Chow R et al.,(2009). Controlling data in the Cloud: Outsourcing computation without outsourcing control, *in proceedings of the 2009 ACM workshop on Cloud computing security. New York, NY: ACM Press: 85–90*

[12] Ristenpart, T., Tromer, E., Shacham, H. & Savage, S., (2009). Hey,you, get off my Cloud: Exploring information leakage in third party computerClouds, *proceedings of the 16th ACM conference on Computer and communications security,07. New York, NY:ACM Press: 199-212*

[13] Cloud Security Alliance, (2010). *Top threats to Cloud computing V1.0. http://www.Cloudsecurityalliance.org/topthreats/csathreats. v1.0.pdf*

[14] RightScale, (2015). *The 2015 state of the Cloud report. www.rightscale.com/lp/2015-state-of-the-Cloud-report*

[15] Hrishikesh, T., (2013). Cloud Adoption Model for Governments and Large Enterprises. Unpublished MSc. Thesis, MIT *available at http://web.mit.edu/smadnick/www/wp/2013-12.pdf*

[16] Oracle (December, 2011). Cloud Computing Maturity model. Guiding Success with Cloud capabilities, white paper *available at http://www.oracle.com/technetwork/topics/entarch/oracle-wp-Cloud-maturity-model-r3-0-1434934.pdf*

[17] Urquhart, J., (2008). A maturity model for Cloud computing, available at http://news.cnet.com/8301-19413_3-10122295-240.html

