University of Nebraska - Lincoln
DigitalCommons@University of Nebraska - Lincoln

Library Philosophy and Practice (e-journal)

Libraries at University of Nebraska-Lincoln

Summer 6-11-2019

CLOUD COMPUTING ADOPTION IN HIGHER EDUCATION: A COMPARATIVE STUDY BETWEEN PUBLIC AND PRIVATE UNIVERSITIES IN SUB SAHARAN AFRICA

VALENTINA ARKORFUL
valentina.arkorful@ucc.edu.gh

CLOUD COMPUTING ADOPTION IN HIGHER EDUCATION: A COMPARATIVE STUDY BETWEEN PUBLIC AND PRIVATE UNIVERSITIES IN SUB SAHARAN AFRICA

ABSTRACT

Cloud computing is fast gaining a significant ground as a solution to offer institutions with competitive advantage compared to the old traditional Technology. Despite the potential benefits that is associated with cloud computing which includes reduction of total costs of acquisition or ownership (TCO) of hardware, software and skilled resources, the adoption level of cloud services is still very low in higher institutions of learning due to security issues, especially trust issues which remain a major concern over cloud solutions. The study was carried out in some selected public and private universities in sub Saharan Africa to determine the reason for the low cloud adoption by key stakeholders in higher institutions of learning. An adoption strategy was recommended with reference to the resources available, confidentiality, integrity and availability. The study recommended that cloud service providers should be transparent with their privacy policies with institutions of higher learning as this can influence cloud purchasing decisions. Secondly, there is the need for training IT personnel and to create awareness of the benefits of cloud computing to enable institutions of higher learning to adopt them to enhance their productivity.

Key words: Cloud computing, TCO, Adoption. Services, stakeholders, resources, Availability, Confidentiality and Integrity.

Introduction

A cloud may be viewed as a large pool of resources put together through virtualization; these resources are handled to dynamically increase proportionally to the load, applying a pay per resources business framework. These resources are made available via a new cloud computing prototype that is being increasingly embraced by modern organisations. The resources include software and hardware on remote data centres, besides services based on those that are reached via the internet (Pearson & Benameur, 2010). Higher education demand for computing needs keeps on changing from time to time. Cloud computing provides higher learning institutions with the opportunity to utilize external providers and on demand services that are highly scalable (Armbrust et. al., 2009) and accessible via internet. The attributes promoted in cloud computing are optimal resource utilization, elasticity, pay per use and multi-tenancy among many other attributes (Agarwal, 2011). According to Cartes (2014) the main concerns on cloud adoption are mainly on safe data management, reliable access control, weak systems monitoring and service availability. Cloud computing is seen as having preceded the technologies required to tackle the trust challenges therefore creating a gap between adoption and innovation (Khan & Malluhi, 2010). Due to this, there is imminent exposure to risks such as theft, leakage of sensitive data and loss of privacy in relation to adoption of cloud computing services (Wang et. al., 2010). These fears are notable in a case whereby in 2007 criminals targeted a well-known cloud computing service provider – Salesforce.com, and managed to steal client information (Omwansa, Timothy & Brian, 2013).

It is advisable that security requirements such as authentication, authorization, availability, confidentiality, identity management, integrity, audit, security monitoring, incidence response and security policy management is addressed by the service provider before providing cloud services. For cloud consumers, delegating some responsibilities to the cloud providers requires some trust and this has been a delimiting condition with cloud service adoption due to such security issues like data loss and surrendering control of data management to the cloud vendor (Zissis & Lekkas, 2012). Adoption consideration for higher institution of learning is not different. With an exponential growth in data traffic ranging from student's registration to access to researched data; IT support requirements for educational, research and innovative activities is enormous. Hence, systems administrators or IT staff in the higher education institutions have to deal with challenges of long-term scalability issues which can be handled very comfortably through cloud. There is the need to find smarter ways to handle the rising demand for data whilst controlling costs. According to Cartes Secure Connexion (2014) results of a Compuware 2014 study shows that 73% of companies do not trust their cloud service providers (this is to say, they were not to delegate their sensitive data to be handled by the cloud service provider); 79% of IT professionals believe that service contracts proposed by cloud computing providers concerning availability do not correspond to risks related to migration and management of cloud applications. Even though, there might be a number of universities using cloud computing, few studies have been conducted on cloud adoption in Sub Saharan Africa. It is with this backdrop that this study seeks to gain an in-depth insight into how key stakeholders view cloud security and trust. The study motivation is to understand what compels the key stakeholders in higher education in evaluating whether to or not to adopt cloud services. The study sought to

1. Find an alternative to the use of Information Technology through cloud, while leading higher institutions of learning to increase operational efficiency and cut cost.
2. Identify key barriers affecting adoption of cloud computing in Higher education in Sub Saharan Africa.

Cloud computing denotes the practice of converting computer services such as data storage and computation to several spare offsite locations available on the internet that enables application software to be applied using internet-enabled devices. In other words, cloud computing offers users and enterprise different potentials to not only process their data but also store it in third party data centres. EDUCAUSE views cloud computing as "the delivery of scalable IT resources over the internet as opposed to hosting and operating those resources locally, such as on a college or university network. It depends on the sharing of resources to get coherence and economies of scale. Underneath cloud computing is the broader construct of converged technology along with shared services (Brown et. al., 2012). Clouds can be categorized as private, hybrid and public (Pearson & Benameur, 2010; CSA, 2011).

This is represented by an SPI Model which is refered to as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The NIST (National Institute of Standards and Technology) defines the service models and deployment models (Ambrust et. al., 2009) as follows:

a) Software as a Service (SaaS)

This is a service that allow the cloud consumer access applications on cloud through an interface (API). The consumer has access to limited control of the application but not on the underlying cloud infrastructure.

b) Platform as a Service (PaaS)

The service allows the consumer to deploy applications onto the cloud infrastructure applications supported by the provider. The consumer has control over the deployed applications and application hosting environment but not the underlying cloud infrastructure.

c) Infrastructure as a Service (IaaS)

This service model provides the consumer with computational resources (networks, storage and processing) to deploy and run software including operating systems and applications. The client has control over operating system environment, storage and deployed applications; little control of networks but not the underlying cloud infrastructure.

Cloud Deployment Models

i. Private cloud:

This is a model for a single organization with various units. Owned and managed by the organization; it may be on or off premises.

ii. Public Cloud:

This is a model for public use. May be owned, managed and operated by a business, academic or government organization or combination. It is off-premise (on the cloud provider side).

iii. Community Cloud:

Model is exclusively for use by a particular group of consumers with a particular interest.

It exists on or off-premise.

iv. Hybrid cloud:

A model combining 2 or more models; but with unique entities. Supports data and application portability (e.g. cloud bursting).

Cloud Reference Model

The Cloud Security Alliance's cloud reference model (**Figure 1**) highlights the relationships and dependencies between the service models (SPI models).

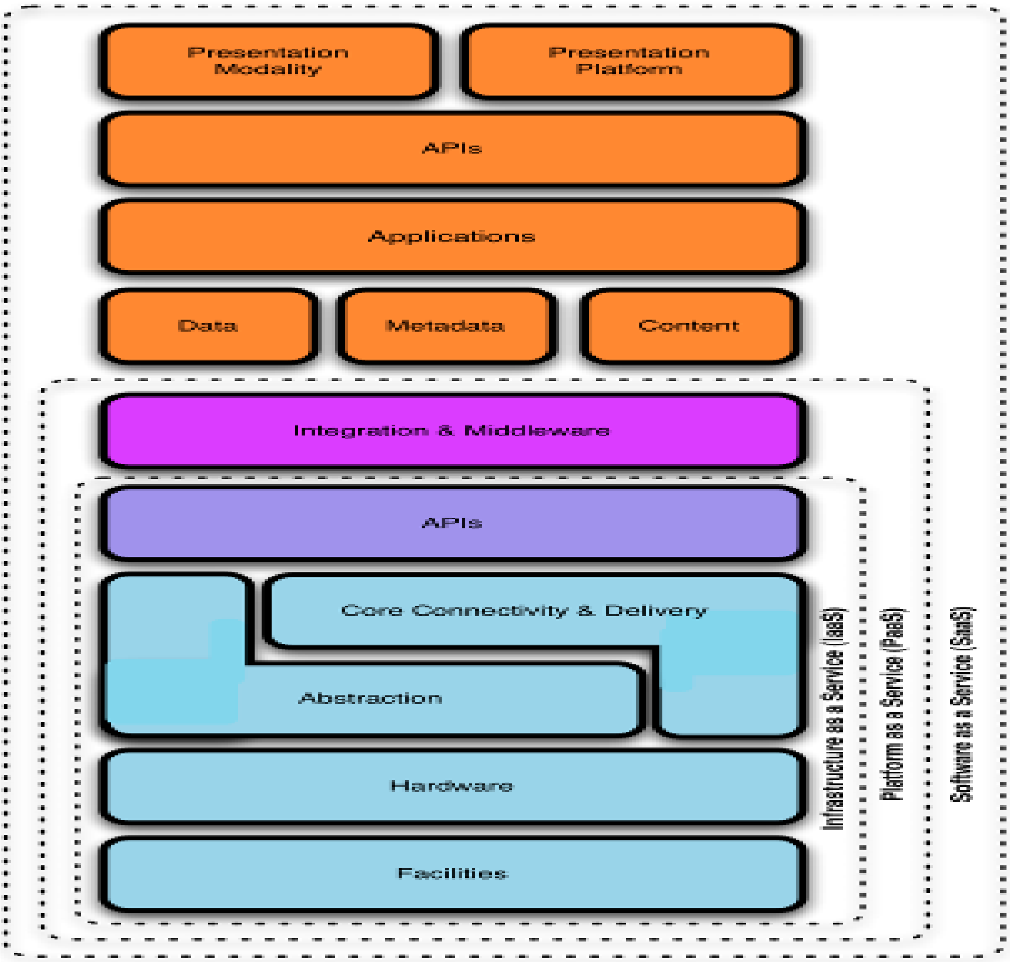


Figure 1. Cloud Reference Model (Source: CSA, 2009

Traditional IT vs Cloud Computing

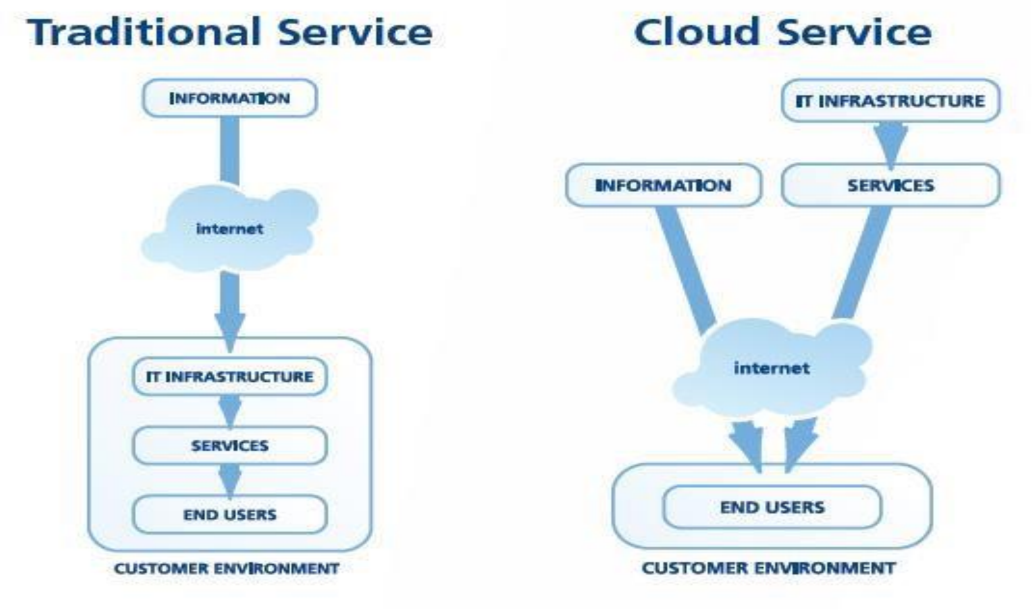


Figure 2: Traditional Service vs Cloud Service (Source: oem.stanford.edu)

Cloud computing facilitates easier system access through internet to users. There is no need of infrastructure locally as the infrastructure provisioned offsite. This is quite useful for higher education institutions in providing Distance Learning facilities and materials to their students in any location without physically attending classes (Cisco, 2011). The other features include cost reductions, reliability, performance and multi-tenancy along with scalability and elasticity (Shelton, 2013; Armburst et al., 2010; Yoo, 2011). Traditional IT services on the contrary are hosted locally (Vijaykumar, 2011) and would not provide the required agility and IT support required for educational research and innovation activities since the high demand requires high investment on hardware, software and skilled service to meet the customers (students & faculty) needs. As such vendors such as Yahoo, Google and IBM are engaged in funding universities to promote cloud computing. These vendors are able to do this through provisioning of hardware, software and services to improve university curricula and expand research horizons for academic communities using cloud computing models (Thomas, 2011)

Benefits of Cloud Computing

The benefits associated with cloud computing are many as indicated in Cisco, white paper: "Cloud Computing in Higher Education - A Guide to Evaluation and Adoption." The two major ones are:

Increased operational efficiency

This improves IT agility and create more room for IT to be innovative. For institutions, it is able to benefit through 'time to market' which means they are able to push products faster in the market. Higher education should bank on this since it gives them a competitive edge to reach a wider or larger market.

Cost cutting

This is achieved through a pay as you go model. The IT Capex is reduced since the infrastructure in use is provided by the Cloud service provider hence no need to invest in software and hardware (Yoo, 2011); it offers flexibility of scaling in and scaling out.

Other benefits are:

i. Ease of deployment of applications: running applications within a short time

ii. Flexibility: opens up opportunity for staff mobility; IT anywhere, anytime

iii. Sustainability: no need to invest in high calibre hardware, software or skilled resources

iv. Staff Redeployment: focus IT on high value tasks

Key Barriers to cloud computing adoption

According to a cloud services survey done by IDC Enterprise Panel, May 2010, the top 3 IT cloud computing concerns are:

i. Security: 87.5%;

ii. Availability: 83.3%

iii. Performance: 82.9%.

Cloud Computing and Trust Issues

According to cloud trust working group within the Cloud Security Alliance (CSA), a trusted cloud is one that a Cloud Service Provider (CSP) implements governance, management and security that meets a minimum set of requirements aimed at increasing confidence of the Cloud Service Customer (CSC). Even though there are benefits linked to speedy and flexible adjustments to service provider's offerings, there is equally high exposure on data privacy and security (Pearson & Benameur, 2010).

According to Booz & Company (2011), there is little visibility in cloud service providers activities for companies whose data are on cloud or moving to cloud and they have a little idea on the kind of security risks exposure faced by the cloud provider. The API interfaces is seen as the possible point of insecurity that could lead to compromise, loss or leakage of data both in storage at the provider and in transit back and forth (Ryan & Falvey, 2012; Bisong & Rahman, 2011). For the health and financial sectors this is the major cause of fear due to the sensitive information dealt with. Due to lack of trust, this would also pose a challenge to larger domains such as institutions of higher learning since they deal with a lot of information or data that is also sensitive. Losing control of their data, would mean they are unable to secure their data from unauthorized access or abuse (Murdoch, 2010).

Trust is a complex construct with many different meanings depending on the context used. Pathan & Mohammed (2015) define trust as a situation where a trustor is willing to depend on the actions of a trustee and therefore has no control of the action or performance of trustee. This situation means the trustor is un-aware of the outcomes or deeds of trustee. A precise definition describes trust as a psychological level made up of risk taking relationships with positive expectations of the intentions or conduct of another (Pearson & Benameur, 2010). Shelton (2013) indicates that the world in general now conducts business on premise of trust alone. In addition, he further argues that adaptability requires the commitment to trust in technological tools that holds information for us.

Weak Trust Relationships

Some levels of frailty may exist in cloud service chain, however, this cannot prevent a service from being offered. Weak API interfaces and sub-contractors are some of the weak links that may exist. API interfaces without proper security mechanism (such as encryption and authentication) in place, this might lead to loss of data, data leakage or even exposure to unauthorized third party access (Awadallah, 2015; Abaddi & Martin, 2011)). The other weak link can occur when a contractor decides to subcontract resulting to numerous business exposure as sub-contractor may not have shared or circulated his data protection standards (Pearson & Benameur, 2010).

Lack of Trust

User's perspective of the cloud service plays a major role in adoption. This is in line with whether the cloud vendor will be able to safely manage or host his data on cloud without interfering with their business. Khan & Malluhi, (2010) highlights elements that directly influence user's level of trust as security, control, ownership and prevention. Furthermore, lack of trust and transparency are mentioned as contributing to the dwindling user trust on cloud services (Agrawal, 2011). In order to enhance users to trust cloud services, Malluhi et al (2010) indicates that a proper remote access control and transparency by service provider on their facilities and action would be pertinent.

Measuring Trust in Cloud

In trust relations, two entities are involved, the trustor and the trustee. In cloud computing context, trustees provide required cloud services and the trustor uses the services provided by the trustee. Huang and Nicol argue that the expected behavior of trustee is out of the trustor's control, however, they should be guided by a core set of values. This means that the trustor will rely on the trustee's capability, goodwill (including intension or motivation) and integrity to guarantee reliable and secure services.

Huang and Nicol highlight several trust mechanisms that can help a cloud user rate cloud services offered by cloud service provider. These are (not limited to the below mentioned):

Reputation based trust

This indicates the entire community view of the cloud service provider. It involves aggregating a large number of peer users rating to determine trustworthiness of the cloud provider. A substantial number of raters is essential for precise and accurate feedback.

Policy based trust

This involves use of Public Key Infrastructure (PKI) authentication. TechTarget.com terms PKI as an enabler between two parties to exchange data over networks such as the internet by use of digital signature and public key certificates that allows authentication. Huang and Nicol suggests that trust in a certification authority as practiced by PKI involves issuance and maintenance of a valid public key certificates based on the certificate authority's conforming to certain certificate policies.

QoS Monitoring and SLA Verification

QoS (quality of service) monitoring verify trust while SLA (service level agreement) verification can be used to adjust trust. QoS monitor tracks performance of the providers; in terms of throughput, response time and availability. SLA will specify details of service metrics agreed upon; it tracks and penalizes any violations in the agreed upon metrics. However, it’s insufficient for invisible elements such as security and privacy.

Evidence based trust

Huang and Nicol highlights attributes for evidence based trust as based on sources of trust (which includes competence, goodwill and integrity) and domain specific goal or objective as envisaged by the trustor.

Cloud Transparency Mechanism

This provides a channel for the cloud user to assess how a cloud provider operates; the only limitation is that the channel is provided by the cloud service provider who might change the data.

Conceptual Framework

Mayers, Davis and Schoorman (1995) trust model illustrates that organization trusts is determined by: the trustee, trustor and perceived risks. We have modified the elements in trustworthiness with Confidentiality, Integrity and Availability which depicts the elements that will influence the user in accepting cloud services as shown in Figure 2.2. A fourth element, on resources was included since it also plays a part in influencing cloud adoption.

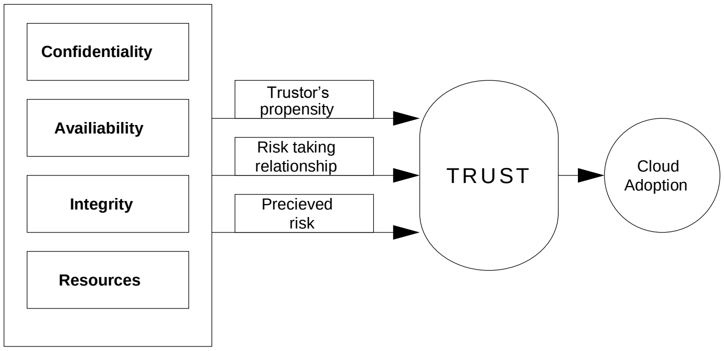


Figure 3: Conceptual Framework for Cloud Service (Source: Inspired by Mayers et al., 1995)

i. According to Mayer et al., *ability* defines competence possessed by trustee in a particular domain; *benevolence* defines the trustees intent to do good for the trustor; and *integrity* determines whether there is a core set of values governing the trustee actions.

ii. In this cloud context, Trustworthiness is replaced by the three security elements which represents the characteristics that the trustee should exhibit; we modified or changed ability with *Availability*-the tendency the trustee will have to ensure that information is accessible to authorized users only and benevolence with *Confidentiality*-ability of the trustee to ensure information is not accessed by unauthorized users or exposed to public.

iii. The trustor will exhibit some perceived risks that is bound to tests current trust. The outcome of the risk taking determines the adoption. This increases or decreases his or her level of trustworthiness, thus influencing adoption or subscribing to cloud services (Mayer et al.).

iv. The propensity of the trustor to trust displays some levels of comfort to work with the trustee. This denotes that some will trust easily but for others an assurance is needed to trust (Mayer et al.). To help us in our study we identified all the key barriers of cloud computing and categorize them based on the key elements (confidentiality, integrity and availability) they affect; resources will help us understand the experience and capability possessed by the trustor. This will help us understand the varied views of key stakeholders that have an impact in cloud adoption or adoption.

Methodology

The study employed the mixed method approach and exploratory research design.With the exploratory design, various sources of information were examined relating to the research problem. This was initiated to create an understanding of trust and adoption issues linked to cloud computing. This form of research design is valuable in secondary data collection, as it gives the researcher a chance to collect essential data from relevant secondary sources that will address the problem (Cohen, Manion & Morrison, 2007). A critical analysis of the secondary research was applied in formulating an adoption strategy and identification of the key barriers of cloud adoption by the key stakeholder in higher education. The dependent variable was the use of cloud computing in institutions of higher education by the key stakeholders (IT Directors/Managers, System Administrators or IT Security personnel); the independent variables focused around 3 key security elements confidentiality, integrity and availability of data. Scores were awarded or assigned per university; evaluation was through a case study. A pragmatic research philosophical approach was used to get credible results through data triangulation of primary data and secondary data.

Target Population

The sample was drawn from a list of public and private accredited universities in Sub Saharan Africa. According to the Commission for University Education (Status of Universities Authorized to operate in Sub Saharan Africa, 2013), there are 22 accredited public universities and 17 accredited private Universities therefore the total number of universities were thirty nine (39).

Out of the 39 Universities (public and private), a sample of 35% was selected, which translated to 13 Universities. A sample size of 10% or more is ideal (Mugenda & Mugenda, 2003) hence, this sample is expected to be a representative of the population. Purposive sampling was used in selecting the respondents for the study. The target respondents were systems administrators, IT Managers/Information Security Managers and other users of the ICT systems.

Data Collection

Cohen, Manion & Morrison, (2007) state that the value of a research work and data collection technique are linked to significantly involving the use of both primary and secondary data. Secondary data according to Sekaran and Bougie (2010) is collected through reviewing existing literature material such as published journals, books and online databases. To assess and ensure secondary data is logical and authentic, it requires to have originated from a precise location and from a confirmable published source. It is pertinent that only well-referenced academic research reports and articles should be considered as secondary data (Cohen, Manion & Morrison, 2007). Based on this argument, it follows that data that was used for this study is from journal articles, books and electronic databases or libraries that are scholarly. Primary data was collected from four (4) IT personnel from each of the thirteen (13) selected universities in Sub Saharan Africa making a total of 52 respondents.

The questionnaire was used as the main primary data collection tool. Creswell and Clark (2011) explain that a questionnaire allows for gathering of large volumes of information within a given time. A preliminary test of the research questionnaire was done specifically for clarity of the research questions.

Table 1: Framework of the interview questions

Objective	Questions	Reason
1. Find alternative to use of IT through cloud, leading higher institution of learning to increase operational efficiency and cut-cost.	The questions under section B on Resources were phrased or directed to assess or measure resource capability of the institution.	This sought to understand the institutional resources capability and skills to see how best the institution can utilize cloud services to cut cost and improve operational efficiency.
2. Identify key barriers affecting adoption of cloud computing in higher education in Sub Saharan Africa.	The questions under availability, integrity and confidentiality guided in collecting the various views and fears of key decision makers in the selected institutions of higher learning.	This sought to identify the main issues influencing the low adoption of cloud services in higher education of learning. This then will be useful in coming up with an adoption strategy or roadmap for increasing adoption of cloud computing in higher institutions of learning.

Data Analysis and Interpretation

The study involved the distribution of fifty (52) questionnaires issued to collect data from 4 IT personnel from the thirteen (13) selected universities. Forty (40) questionnaires from ten universities were filled by the respondents and returned for analysis giving a response rate of 76.9 %. This response rate was considered adequate for analysis to determine the usage of cloud computing in higher education in Sub Saharan African public and private universities. According to Awino (2011), a response rate of 65 percent is acceptable for such studies and hence the response rate of this study was representative of the universities as far as this study was concerned. The responses are captured in the table below as per their institution and department . The respondents were to respond to questions on availability and reliability of infrastructure and productivity levels. They were also asked to respond to their resource skills capability, whether there are plans to adopt cloud computing and their current adoption level. They also responded on the confidentiality and integrity of the policies for purchasing cloud computing resources and ranked cloud computing services and their efficiency for service delivery.

Table 1: Company/Institution * Section/Department Cross tabulation

	Section/Department	Academics	Computer Science	ICT	IT	Multimedia	Network	Total
University	1	0	0	4	0	0	0	4
	2	0	0	1	3	0	0	4
	3	0	2	1	1	0	0	4
	4	0	0	4	0	0	0	4
	5	0	0	1	3	0	0	4
	6	2	0	2	0	0	0	4
	7	0	0	4	0	0	0	4
	8	0	0	4	0	0	0	4
	9	0	0	2	0	0	2	4
	10	0	0	3	0	1	0	4
Total		2	2	26	7	1	2	40

From table 1., two of the respondents were from the academics department, 2 were from computer science,7 from IT, 1 from the multimedia department, 2 from networking department and majority (26) from the ICT department. This resulted in a total of 40 respondents as per the questionnaires that were returned from the analysis.

Personal Information on years of experience of respondents

The respondents were asked to provide information on their years of experience and they responded as shown in Table 2 below.

Table 2 : Statistics on the years of experience

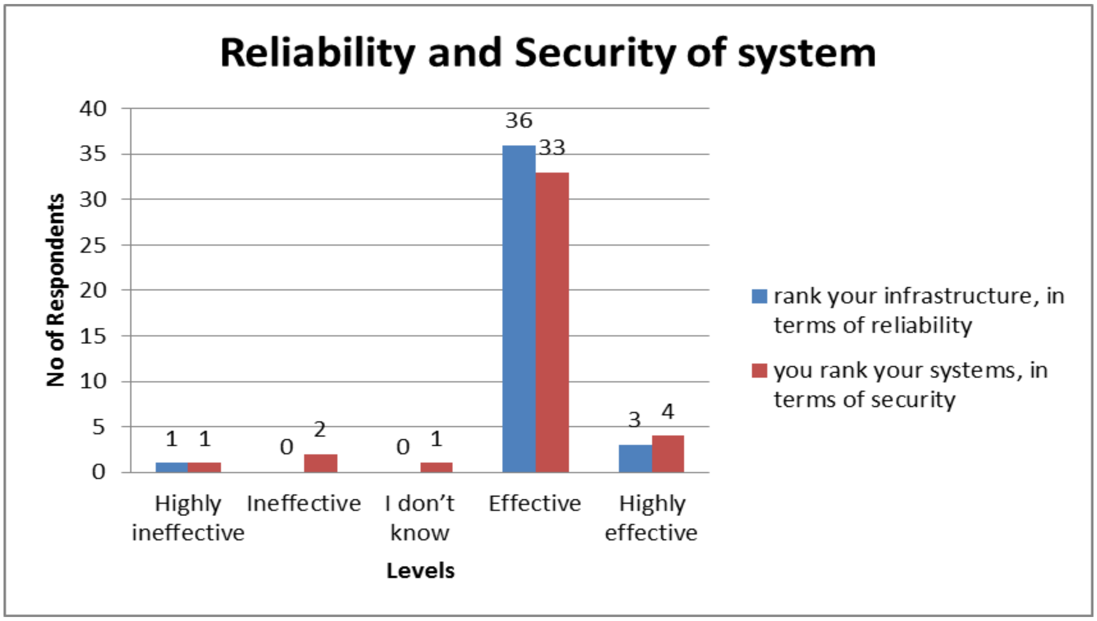
	N	Range	Minimum	Maximum	Mean	Std. Deviation
Years of Experience	40	13	1	14	5.17	2.854
Valid N (Listwise)	40					

From Table 2, majority of the respondents had worked for an average of 5.17 years which portrayed their experience in their position of service in these institutions. Some employees had maximum experience of 14 years and some had minimum experience of 1 year. The standard deviation was 2.854 which indicates that majority of employees had almost the same experience on the average and this indicated that the employees were in a position to give more reliable and valid information on the usage of cloud computing in higher education in Sub Saharan Africa.

Availability

This is the tendency that the trustee will have to ensure that information is accessible to authorized users only. This is in line with the reliability and security of the systems used in these universities. The results on the reliability and security of the systems are presented in the multiple bar charts below.

Figure: 4 Bar-chart of Reliability and security of the systems.



From Figure 4, one of the respondents ranked both infrastructure in terms of reliability and system security as highly ineffective. Two of the respondents ranked them as ineffective to their systems in terms of security, onerespondent did not know whether their system is secure or not. Majority of the respondents (36) ranked their infrastructure to be effective in terms of reliability and 33 ranked their systems effective in terms of security. For those who indicated that they were highly effective, 3 suggested that the availability of infrastructure in terms of reliability is highly effective and 4 indicated that system in terms of security was highly effective. This indicated that majority ranked the infrastructure reliability and system security to be effective and hence always available for their services.

Cloud services

The respondents were requested to suggest the type of cloud services hosted on cloud and they responded as shown in the table below.

Table 3 IaaS * Functions hosted on cloud Cross tabulation

Count	any of your functions hosted Strongly Agree	Somehow agree	on cloud Not Sure	Somehow disagree	Strongly disagree	Total
	12	11	1	4	8	36
IaaS	2	2	0	0	0	4
Total	14	13	1	4	8	40

From Table 4.3, Majority being 14 of the respondents strongly agreed that they have functions or services hosted on cloud, 13 somehow agreed, 1 was not sure, 4 somehow disagreed and 8 strongly disagreed. Incidentally, only 4 respondents knew the type of cloud service model they were using. This indicates that some of the users do not know the type of cloud service model in use and some institution have not yet hosted any function on the cloud service. This means there is the need for the technical staff in these institutions to familiarize themselves with the various cloud service models and deployment models in order to increase their operational efficiency and find viable ways they can cut cost by hosting some of the services on cloud. Some of the functions highlighted to be hosted on cloud includes file based storage (mail), management information system, faculty management system, Google apps, virtualized services and student management systems.

Functions Hosted on cloud

The respondents were requested to indicate the functions hosted on cloud and they responded as in the table below

Table 4: Frequency table of functions hosted on cloud

	Frequency	Percent
Strongly Agree	14	35.0
Somehow agree	13	32.5
Not Sure Somehow	1	2.5
disagree	4	10.0
Strongly disagree	8	20.0
Total	40	100.0

From table 4.4, 35% of the respondents strongly agreed that at least their services are hosted on cloud, 32% somehow agreed, 2.5% were not sure, 10% somehow disagreed and 20% strongly disagreed. This indicates that 67.5% agreed that they host their services on cloud and it this indicates that some of the institutions have already seen the benefits associated with cloud computing such as increase in operational efficiency, low cost, ease of deployment of applications etc.

Cloud Services on Increase of productivity

The respondents were requested to indicate in their views if cloud services increase their productivity and they responded as in the chart below.

Figure: 5 Bar-chart of cloud services and productivity.

Figure: 5 Bar-chart of cloud services and productivity.

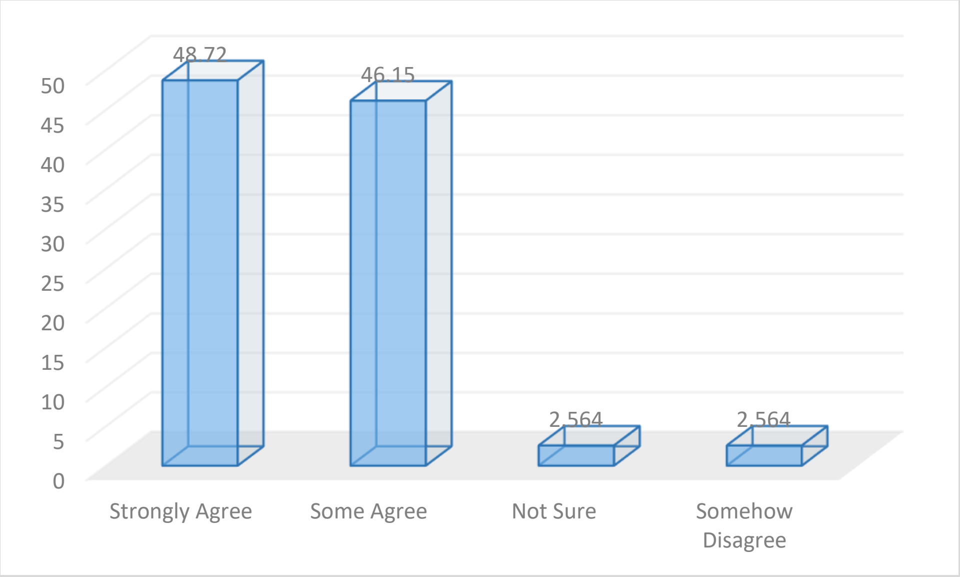


Figure: 5 Bar-chart of cloud services and productivity.

From Figure 5, 2.56% of the respondents somehow disagreed and others were not sure if the cloud services increase their productivity. Majority being 48.72% strongly agreed, 46.15% somehow agreed that these services increase their productivity. This is an indication that cloud computing will enable flexibility and free up human resources especially IT staff to focus on high value tasks leading to high operational efficiency. As a result, due to high available systems, this will increase staff performance leading to high productivity.

Integrity

This is a scenario observed in institutions that entails whether the trustee has a core set of values to guide behavior. This was to enable in formulating a strategy that addresses trust issues in the adoption of cloud services in Sub Saharan African public and private universities. The integrity in this study was a discussion in the following sections:

Strategies observed on integrity

The respondents were asked on how they rated cloud services, how cloud services lead to operational efficiency, and their opinion on whether hosting data on cloud is secure and they respondent as in the table below.

Table 5 Rating of cloud Services

	N	Mean	Std. Deviation	Std. Error Mean
How would you rate cloud services to any organization	39	3.82	.854	.137
would cloud services leads to operational efficiency	39	1.87	1.056	.169
is data hosted on cloud secure	35	2.37	1.140	.193

From table 5, the rating of cloud services in the institution had a mean of 3.82 which is close to 4 and hence it's effective as per the Likert scale used. A standard deviation of .854 which indicates that majority of the respondents had a common response of accepting that the usage of the cloud services in their institution is effective. Hence this indicates a high confidence in cloud services which is worth implementing. Cloud services leading to operational efficiency in institutions had a mean of 1.87 which is close to 2 and hence it's somehow agreed a standard deviation of 1.056 however indicated that majority of the respondents had a common response of accepting that cloud services lead to operational efficiency. Data hosted on cloud being secure had a mean of 2.37 which is close to 2 and a standard deviation of 1.140 indicated that majority of the respondents had a common response that data hosted on cloud is secure.

Stumbling blocks to cloud service adoption

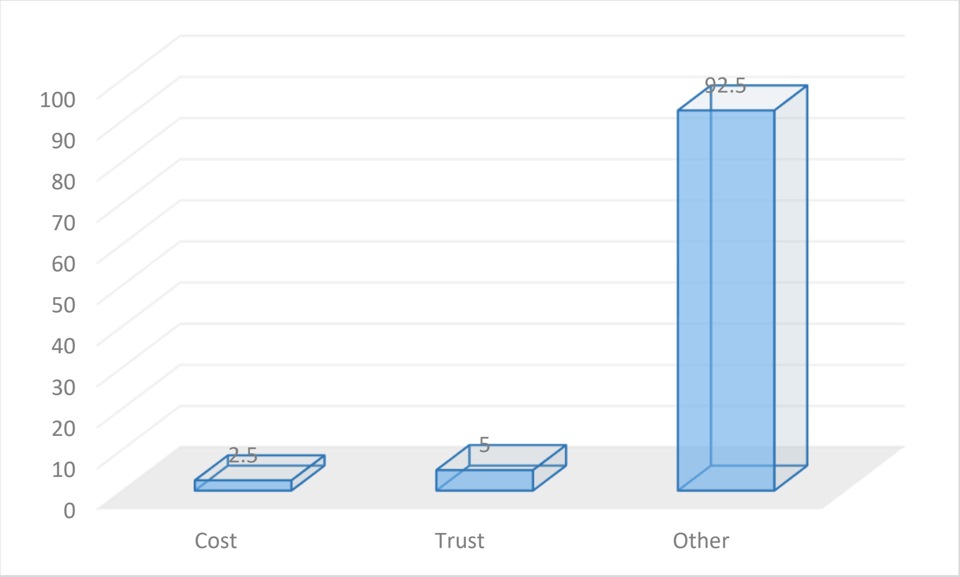
Table 6: One-Sample Test on stumbling blocks to cloud services adoption

Components	t	df	Sig. (2-tailed)	Mean
Loss of control of data	27.324	28	.000	4.310
Privacy	31.165	30	.000	4.194
Data Leakage / Loss	14.809	30	.000	3.613
Security	22.919	27	.000	4.071
Compliance Issues	20.600	26	.000	3.815
Contractual Issues	22.718	23	.000	4.083

Availability	25.720	24	.000	4.200
Performance	18.207	22	.000	4.043
Data Portability	/			
migration Issue	22.277	24	.000	3.960
Lack of standards	11.694	22	.000	3.435
legal issues	10.834	20	.000	3.426

From table 6, Loss of control of data had a mean of 4.310 which is close to 4 which indicates that loss of control of data is a stumbling block to cloud service adoption. Privacy had a mean of 4.194 indicating that Privacy is a stumbling block to cloud service adoption. Data Leakage / Loss had a mean of 3.613 indicating that Data Leakage / Loss is a stumbling block to cloud service adoption. Security had a mean of 4.071 meaning that security in general is a stumbling block to cloud service adoption. Compliance Issues, Contractual Issues, Availability, Performance, and Data Portability / migration Issue had (mean≥3.5) meaning they are stumbling blocks. Lack of standards and legal issues had (mean≤3.5). All the components of investigation had a significant value at p<.05 and this suggest that they had significant effect on cloud service adoption. The respondents indicated that other stumbling block include cost and trust as indicated in the pie-chart below

Figure 6: Pie-Chart for other stumbling blocks in cloud computing



From Figure 6, 2.5% indicated that cost was a stumbling block, 5.0% indicated that trust was a stumbling block to cloud services adoption. The remaining majority did not suggest other stumbling blocks.

Cloud Service Providers

The respondents were asked to respond on whether the cloud service providers have the capability and skills to handle their institutions data and they responded as in the figure below.

Table: 7 Cloud Service Provider capability and Skills

	Frequency	Percent
Strongly Agree	9	22.5
Somehow agree	21	52.5
Not Sure	1	2.5
Somehow disagree	3	7.5
Strongly disagree	6	15
	35	100
Total	40	100.0

From table 7, 22.5% of the respondents strongly agree that the cloud service providers have capability and skills to handle any of their institution data, 52.5% confirmed that they somehow agree that the cloud service providers have the capability and skills of handling their institutions data. Those who were not sure were 2.5%, 7.5% disagreed and 15% strongly disagreed. In general 75% of the respondents agreed that cloud service providers have the skills and capability to handle their institutional data. This indicates that some institutions do not trust the skills and capability of the cloud service providers to handle their institution data. Thus one strategy should be to encourage information technology staff in these institutions to work together with the cloud service providers in order to develop trust in the cloud service provider’s ability to handle hosted services; this will improve the usage or adoption of cloud computing in higher learning institutions in Sub Saharan Africa.

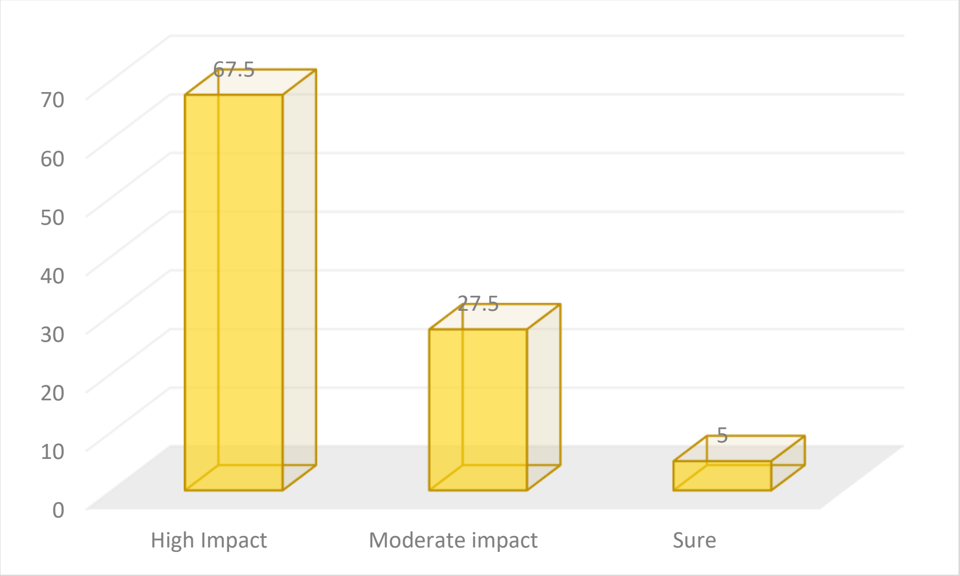
Confidentiality

In this section the respondents were asked about issues on confidentiality of the services offered in these institutions. These included issues on cloud provider's privacy policy, security and threats, response to security and threats, service level agreement and adoption process in institutions of higher learning in Sub Saharan Africa. All these were discussed as follows.

Impact of cloud provider's privacy policy

The respondents were asked to give their views on impact of cloud provider's privacy policy on their institutions cloud purchasing decision and they responded as in the figure below,

Figure 4: Bar-chart of the impact of cloud provider's privacy policy



From Figure 4, majority of the respondents, 67.5% accepted that the impact is high on institutions cloud purchasing decisions, 27.5% accepted that it had a moderate impact and 5% were not sure. The study indicated that about 95% agreed on high impact on cloud purchasing decision. This impact is a key barriers affecting adoption of cloud computing in Higher education in Sub Saharan Africa.

Security Threats associated with cloud computing.

The respondents were asked to give their views on security threats associated with cloud computing and they responded as shown in the table below

Table 8: One-Sample Test on views on security threats

	T	df	Sig.	(2-tailed) Mean
Data Loss	16.681	38	.000	3.821
Services & data unavailability	15.583	36	.000	3.676
Privacy	20.306	39	.000	4.100
Shared technology vulnerability	17.233	38	.000	3.615
Security (application security, controls)	17.766	39	.000	3.750
Vendor Lock-in	16.523	39	.000	3.500
Hypervisor vulnerability	15.628	39	.000	3.125
Insecure API's	17.160	39	.000	3.475

From table 8, Data Loss had a mean of 3.821 which is close to 4 indicatimg that data loss is a security threat associated with cloud computing and has high security threats which can hinder the adoption of cloud services. Services & data unavailability had a mean of 3.676 which means that unavailability of services & data has a high security threat rate which can hinder the adoption of cloud services. Privacy had a mean of 4.100 and shared technology vulnerability had a mean of 3.615 meaning that Shared technology vulnerability is a security threat associated with cloud computing and has high security threats which can hinder the adoption of cloud services. Security (application security, controls) and vendor Lock-in had (mean≥3.5. Hypervisor vulnerability and legal issues had (mean≤3.5, security threats associated with cloud computing had a moderate effect in hindering the adoption of cloud services. All the views on security threats associated with cloud computing had a significant value at p<.05 and this suggests that the threats had a significant influence on the adoption of cloud services.

How Universities handle security threats.

The respondents were asked to give their views on how their university handle security threats and they responded as shown in the table below:

Table 9: Statistics on response to security

	Reporting incidences	Incidence Response Management	Threat & Vulnerability Management	Identity & Access Management
N	39	36	39	38
Missing	1	4	1	2
Median	4.00	4.00	5.00	4.50
Mode	5	4	5	5
Std. Deviation	1.341	1.082	1.063	1.053
Range	4	4	4	4

From table 9, Reporting incidences had a mode of 5 indicates that reporting incidences is very a frequent way of how these institutions handle security threats. Incidence Response Management had mode of 4 , Threat & Vulnerability Management had mode of 5, Identity & Access Management had mode of 5 pointing to the fact that identity & access management is a very frequent way of handling security threats.

Visibility, Accountability and Transparency

The respondents were asked to give their views on the visibility, transparency of cloud service provider and they responded as follows.

Table 10: visibility, accountability and transparency

	N	Mean	Std. Deviation	Std. Error Mean
Is there visibility over the cloud services being offered by the cloud service provider	39	2.08	.664	.106
Is there need to hold service providers accountable based on the service level agreement signed.	40	1.10	.304	.048

Transparency of the cloud service operations might influence the cloud adoption process within the institution.	40	1.43	.501	.079

From table 10, there is visibility over the cloud services being offered by the cloud service provider had a mean of 2.08, this indicates that majority of the respondents somehow agree that there is visibility over the cloud services being offered by the cloud service provider. Accountable based on the service level agreement signed had a mean of 1.01 indicating that majority of the respondents strongly agree that there is need to hold accountable the cloud service providers based on the signed service level of agreement. Transparency of the cloud service operations might influence the cloud adoption process within the institution since it has a mean of 1.43 which is close to 1 which is strongly agree from Likert scale. This indicates that majority of the respondents strongly agree that transparency over the cloud services being offered by the cloud service provider will influence the adoption rate of cloud services in their institutions.

Resources

In this section the respondents were asked about the resources in their institutions the responses are indicated in the Table below.

Table 11 Resources

Resources	N	Mode	Std. deviation	Range
Have enough resources and skills to manage your systems inhouse	40	1	1.011	3
Their average working experience	40	2	.516	2
Is cloud computing significant to your institution	40	1	1.071	3
There are plans to adopt cloud computing fully as a cost cutting venture and to bolster operational efficiency	40	2	.975	3

What stage is your institution in with regard to cloud services adoption	40	1	1.095	3

From table 11, the institutions have enough resources and skills to manage their systems in-house, average working experience had a mode of 2 which is somehow an indication that majority of the respondents somehow agree that the institutions have average working experience. Majority of the respondents indicated that they strongly agree that cloud computing is significant to their institutions.Majority of the respondents somehow agreed that their institutions plan to adopt cloud computing fully as a cost cutting venture and to bolster operational efficiency in their institution.Majority of the respondents agreed that their institutions were already in use/implementation stage with regards to cloud adoption.

Reliability and Validity of the Study

The independent variables in the study were tested on their reliability and validity to be included in the study. The independent variables are availability, integrity, confidentiality and resources on cloud computing in the universities. The analysis was displayed as per the table below.

Table 12 Reliability and Validity

Independent variables	Cronbach's Alpha
Availability	.702
Integrity	.707
Resources	.754
Confidentiality	.890

From the table 4.12, it indicates that the Cronbach's Alpha for all the independent variables is >0.7 and this indicates that they were reliable to be applied in any location to collect the data. This made the questionnaire to be more reliable for the study.

Statistical analysis of effects of independent variables on Cloud Adoption

To test the moderating effect on the relationship between the independent variables (availability, confidentiality, integrity and resources) on dependent variable (cloud adoption), we used the T test sample (Table 13) and regression analysis as a comparison (Table 14).

Table 13 One-Sample Test of Independent variables

	Test Value = 0					
	t	df	Sig. (2tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Resources	21.692	39	.000	1.892	1.72	2.07
availability	41.081	39	.000	3.019	2.87	3.17
Confidentiality	33.744	39	.000	3.202	3.01	3.39
Integrity	32.753	38	.000	3.392	3.18	3.60

From the t-test table the p-value at two tail <.05 hence it indicates that the availability, confidentiality, integrity and resources had significant influence on the adoption of cloud computing in the institution of higher learning in Sub Saharan Africa .

Table 14:Regression analysis table on effects of dependent and independent factors

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	.312	1.670		.187	.853
availability2	.295	.338	.127	.875	.388
Confidentiality2	-.548	.257	-.302	-2.131	.040
Integrity2	.188	.246	.111	.766	.449
Resources	1.042	.284	.525	3.666	.001

a. Dependent Variable: Cloud adoption

From the table, the regression equation for the effect of resources, availability, confidentiality and integrity on adoption of cloud computing was derived as follows:

Cloud adoption=.312 (constant) +.295*availability -.548*confidentiality +.188*integrity +1.042*resources. From the table only the effects of confidentiality and resources were significant at p<.0.05. Availability, resources and integrity had positive effects whilst confidentiality had a negative effect on adoption of cloud computing in universities in Sub Saharan Africa.

Conclusions

The following conclusion was reached following the analysis of the statistical data collected from the respondents.

1. With regards to "Find alternative to use of IT through cloud, while leading higher institutions of learning to increase operational efficiency and cut cost."

The study concludes that there is a growing receptiveness of cloud computing services in the institution of higher learning. 67.5% host services on cloud but only 10% know the type of cloud model used by their institution. Infrastructure as a Service (IaaS) is the cloud model used by many of these institutions. This means that there is the need for these institutions to ensure that their information technology team are well verxed with the changing technology trends such as cloud computing (this can be facilitated through sponsoring them for cloud computing workshops, seminars or even through technology benchmarking) to be able to acquire necessary knowledge on the various cloud computing models and deployment. This will help them to identify a viable solution that will meet the on-demand service requirements for their institutions and thus aid in reducing cost and increasing operational efficiency in their institutions. The study concludes that cloud computing is rated highly by the institutions of higher learning as a way of enhancing operational efficiency and cutting cost. Majority of the respondents had a mean of 3.82 which is denoted "effective". Majority of the respondents also indicated that data hosted on cloud is secure. Availability of data or services through reliable infrastructure and secure systems is key for the institutions to work and would therefore play a major role in cloud adoption. 36 respondents ranked their infrastructure as effective in terms of reliability and 33 respondents ranked their system effective in terms of security; 3 respondents indicated that their infrastructure was highly effective while 4 indicated that their system security was highly effective.

95% of the respondents cumulatively agreed that cloud computing services increase productivity. This means that cloud services will aid in enhancing the performance of institutions of learning through technology leverage thus creating a competitive advantage. It is also likely to address scalability issues and increase IT agility to support these institutions effectively and efficiently.

2. With regard to "Identifying key barriers affecting the adoption of cloud computing in Higher education in Sub Saharan Africa."

The study concludes that loss of control of data, availability, privacy, contractual issues, security, performance, data portability/migration issues, compliance issue, data leakage/loss, lack of standards and lastly, legal issues are the main barriers to cloud computing adoption in institutions of higher learning from the topmost level to the bottom level.

Other stumbling blocks are cost and trust which are at 2.5% and 5% respectively; 92.5% of the respondents did not indicate other stumbling blocks to cloud adoption. This number could fall on either of the two sides; hence, further studies need to be conducted to ascertain the extent to which cost and trust influence the low adoption of cloud computing in institutions of higher learning.

The study also concludes that the cloud provider should be held accountable based on the cloud service provided to the cloud user, transparency of the operations on cloud services provided and adherence to privacy policy. This will have a big impact on cloud purchasing decisions resulting in increased adoption of cloud services. 95% of the respondents agreed that there is an impact on cloud provider's privacy policy on cloud purchasing decisions. From the study, privacy tops in the list of security threats with a mean of 4.1. Hence, cloud service providers have a mandate to protect the privacy and security of data they are managing on behalf of the institutions.

3. With regard to "Develop a strategy or roadmap for adoption of cloud computing in Higher Education in Sub Saharan Africa."

All objectives were met resulting to a formulation of strategies to be used by higher education institutions of learning while implementing cloud services. The roadmap was formulated based on the identified key barriers to cloud computing in institutions of higher learning. Participation or support of the top management is key for the success of roadmap.

Recommendations

Cloud service providers should be transparent with their privacy policies with institutions of higher learning as this can influence cloud purchasing decisions. Secondly, there is the need for training and the creation of awareness of cloud services through workshops and seminars.

REFERENCES

Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, *16, 108-114.*

Abdulsalam, G. & Fatima, Z (2011) "Cloud Computing: Solution to ICT in Higher Education in Nigeria", *Pelagia Research Library Communications of the ACM, Vol. 51 p. 9-11*.

Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, *1 (Special Issue on CNS), 257-259*

Armbrust, M. Fox, A, Griffith, R. Joseph, D. A. Katz, R. Konwinski, (2009) A. Above the clouds: *A Berkeley View of cloud computing*.

Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), *30-45.doi:10.5121/ijnsa.2011.3103*

Bryman, Awino (2011).*Business research methods*. Third edition Oxford: Oxford University Press.

Cohen, L, Manion, L & Morrison, K 2007, *Research methods in education* (6th Ed.). London: Routledge.

Creswell, J, & Clark, V 2007, *Designing and conducting mixed methods research*. Thousand Oaks: Sage Publications.

Grossman, R.L. (2009). The Case for Cloud Computing. IT Professional [Electronic], 11(2), pp.23–27.

Hashizume et al. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, *4(5), 1-13*.

Khan, M & Malluhi, Q, 2010, Establishing trust in cloud computing, *IT Professional Magazine*, 12(5), 20-27,

Khorshed, T.M., Ali, A.B.M.S. and Wasimi, S.A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems, 28, 833–851.*

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011).Cloud computing — The business perspective. Decision Support Systems, 51, 176–189.

Mircea, M. & Andreescu, A. J. (2011). "Using Cloud Computing in Higher Education: A strategy to improve agility in the current financial crisis", *Academy of Economic Studies, Bucharest, Romania.*

Mugenda, O. M. and Mugenda, A. G. (2003).Research methods: quantitative and qualitative approaches. Nairobi. Acts press.

Mugenda, O. M. and Mugenda, A. G. (2008).Research methods: quantitative and qualitative approaches. Nairobi. Acts press

Omwansa, T, Timothy, W & Brian, O 2013, Cloud Computing in Kenya, *A 2013 Baseline Survey*

Pearson, S & Benameur, A 2010, Privacy, Security and Trust issues arising from cloud computing, *2nd IEEE international conference on Cloud Computing Technology and Science*.

Ryan, P. and Falvey, S. (2012). Trust in the clouds. Computer Law and Security Reviews, 28, *513-521.*

Roberts, J & Al-Hamdani, W 2011, "Who Can You Trust in the Cloud? A Review of Security Issues within Cloud Computing", *Information Security Curriculum Development Conference 2011*, ACM, 15-19.

Schyff, K & Krauss, K 2014, Higher education cloud computing in South Africa: Towards understanding trust and adoption issues, *SACJ*, 55, 40-54.

Sekaran, U & Bougie, R, 2010, *Research methods for business: A skill building approach.* New York: John Wiley & Sons.

Shelton, T 2013, *Business models for the social mobile cloud*, John Wiley & Sons.

Sun, D, Chang, G, Sun, L, & Wang, X, 2011, Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments, *Procedia Engineering*, 15, 2852-2856,

Weinman, J 2012, *Cloudonomics: The business value of cloud computing*. New York: John Wiley & Sons.

Zissis, D and Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28, 583–592*.