USING CLOUD COMPUTING IN HIGHER EDUCATION: A STRATEGY TO ADDRESS TRUST ISSUES IN ADOPTION OF CLOUD SERVICES IN KENYAN PUBLIC AND PRIVATE UNIVERSITIES

BY

DANIEL OCHIENG ONYANGO

P54/72808/2014

A Research Project submitted to the University of Nairobi in partial fulfilment of the requirements for award of Master of Science Information Technology Management Degree

SUPERVISOR: PROF. ELIJAH OMWENGA

NOVEMBER 2016

DECLARATION

This project is my original work and has not been presented for award of a degree in any university.

Signed…… Date……

Daniel Ochieng Onyango

Reg No: P54/72808/2014

This proposal has been submitted for examination with my approval as the University Supervisor.

Signed…… Date……

Professor Elijah Omwenga

School of Computing and Informatics

University of Nairobi.

ABSTRACT

Cloud computing is fast gaining significant ground as a solution to offer institutions with competitive advantage compared to the old traditional IT. Nevertheless, many institutions are still clenched to the traditional IT where legacy IT systems or applications are hosted in-house and hence administration of the systems or services is local or on- premise. This has resulted in high IT expenditures on both hardware and software due to increased storage demands as well as investing on high skilled resources to administer the existing systems or applications which might not be viable in the long run. There are three main service models of cloud computing which through them other service models have been derived. SPI Model, as it is known comprises of Software-as-a service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). Deployment of these services can be through Public Cloud, Private Cloud, Hybrid or Community Cloud depending on the services or applications used by the institution. 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, adoption level of cloud services is still very low in higher institutions of learning due to matters security especially trust issue which remains a major concern over cloud solutions. A case study was carried out in selected public and private universities to determine the reason for the low cloud uptake by the key stakeholders in higher institution of learning. An adoption strategy was recommended with reference to the resources, confidentiality, integrity and availability. The focus was on how key stakeholders view cloud services in the context of unique operational efficiency.

DEDICATION

To my family and all my friends who were there to encourage and support me. I dedicate this work to you.

To God be the Glory.

ACKNOWLEDGEMENTS

First and foremost, my appreciation to Almighty God for granting me the ability, wisdom and strength to complete this dissertation.

Am very grateful to my supervisor Prof. Elijah Omwenga for his constant support, guidance and unending patience; through your encouragement and guidance you made my completion of this dissertation possible.

Special thanks goes to Dr. Christopher Moturi for his un-ending support and encouragement; am also very grateful to the panel who sat patiently to listen to us and to guide us. My humble appreciation to all those who helped me during data collection, validation and analysis of data.

Finally, to my wife Catherine, daughter Vanessa, Mum, Dad and all my siblings, thank you all for the endless support and encouragement.

ABBREVIATION

Abbreviation	Description
API	Application Programming Interface
CAPEX	Capital Expenditure
CSA	Cloud Security Alliance
CSC	Cloud Service Consumer
CSP	Cloud service Provider
IaaS	Infrastructure as a Service
IBM	International Business Machine Corporation
ICT	Information Communication Technology
IDC	International Data Corporation
IT	Information Technology
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
PKI	Public Key Infrastructure
QoS	Quality of Service
SaaS	Software as a Service
SLA	Service Level Agreement
SPI Model	Software as a Service; Platform as a Service; Infrastructure as a Service Models
SPSS	Statistical Package for the Social Science
TCO	Total Cost of Ownership

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION TO STUDY

1.1. Introduction

Cloud computing is a rising paradigm for organizations in the contemporary world. There are benefits associated with it such as cost cutting resulting from shared computing resource that include storage resource together with an on-demand mechanism that promotes a pay per use model (Pearson, S & Benameur, A 2010). These new aspects have a direct effect on information technology budgeting, trust, traditional security and privacy mechanisms. A number of these mechanisms are no longer enough, but ought to be considered to fit this new paradigm. The NIST (Mell& Grance, 2011) defines "cloud computing as a model that enable ubiquitous convenient, on demand network access connecting to a pool of shared configurable computing resources. This research study explore on how trust as a factor influences decision to adopt cloud computing in higher education in Kenya and ways in which such issues may be addressed.

1.2. Background of Study

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 these that are reached via the internet (Pearson, S & Benameur, A 2010). Higher education demand for computing needs keeps on changing from time to time. Cloud computing provides them with the opportunity to utilize external providers and on demand services that are highly scalable (Armbrust et. al., 2009; Rimal 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 (Reese, 2009; Agarwal, 2011; Pathan & Mohammed, 2015; CSA. 2011). These attributes provide the means to power large infrastructure like data centres via virtualization and resource management. Virtualization and automated bare-metal are technologies that supports cloud computing at the back-end (Weiman, 2012; Zissi & Lekkas,

2012; Zheng, 2011; Brown et. al., 2012). However, these large pools of resources are not located in the same geographical region (Bisong & Rahman, 2011; Khorshed et. al., 2012). Moreover, the vibrant increase or shrinking of cloud makes it daunting to check on deployment and on the location hosted or the geographical area ((Tenayuca, 2011; Khan & Malluhi, 2010). This makes compliance with set rules on data handling challenging to meet (Pearson & Benameur, 2010).

Cloud utilization requires users or organizations to trust the cloud providers. This is however not the case as main concern revolves around security, privacy (Bisong & Rahman, 2011; Hashizume et. al., 2013) and reliability (Khorshed & Wasimi, 2012) affecting adoption especially in the professional realm. According to Cartes Secure Connexion 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). This research study looked into higher education cloud computing in Kenya: A strategy to address trust issues in adoption of cloud computing in higher education.

1.3. Statement of the Problem

According to Fang et al., the cloud consumer is the main stakeholder for cloud services. The cloud consumer may either be a person, company or organization who is billed for utilizing cloud services provisioned by the cloud provider. 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 and Lekkas, 2012). Adoption consideration for higher institution of learning is not different. With an exponential growth in

data traffic ranging from students 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 need to find smarter ways to handle the rising demand for data while at the same time 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 research has been done related to trust and cloud adoption in Kenya. It is with this backdrop that this study seek to gain in-depth insight into how key stakeholders view cloud security and trust. The study motivation is to understand what compels the key stakeholders in the higher learning education in evaluating whether to or not to adopt cloud services. From the available literature reviews, there are few existing studies that focus on cloud computing adoption and trust within the higher education in Kenya.

1.4. Research Objectives

The main research objectives for this study are:

1. Find alternative to use of IT 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 Kenya
3. Develop a strategy or roadmap for adoption of cloud computing in Higher Education in Kenya.

1.5. Justification of Study

Information security concerns are still the major issue in adoption of cloud computing in Kenya; about 39% more organizations uses pure private cloud compared to 29% who uses public cloud (Omwansa, Timothy & Brian, 2013). The biggest consumers are financial sectors followed by telecommunication sectors; education and government have been named as moderate users of

cloud, which is not clear what percentage of university utilizes either private or public cloud. The choice is mainly as a result of concerns around security and control of access of organizational data (Omwansa et al.). This is confirmed by Roberts & Al-Hamdani (2011) who indicate that fear on confidentiality, availability and integrity of information have been the major propelling force for slow cloud adoption rate; the question mainly asked is, "how can the customer trust the provider's management of the data?" This is a clear indication of concern with loss of control on data. Schyff and Krauss did a similar research but in South African Higher education context; their findings showed that trust in cloud security is either internal or external to the university. Stakeholders are depicted to make judgements about whether cloud services can be trusted based on how cloud security is evaluated. Their differing views are attributed to loss of control of cloud-based data (Schyff & Krauss, 2014). This study is justified to provide insight into the issue of low cloud services uptake and enable those responsible to embrace effective strategies in the successive adoption and management of cloud computing in the higher education sector.

1.6. Research Question:

1. What are the other alternatives to use of IT that is geared towards increasing operational efficiency and reducing cost in higher education in Kenya?
2. What are the key barriers influencing decisions to adopt cloud computing by the Key stakeholders in higher education in Kenya?
3. Can adoption strategy improve or increase cloud uptake in higher education?

1.7. Assumptions:

The cloud consumer in this case, the institution of higher learning has one or more functions hosted on cloud. The cloud provider was transparent on matters relating to information security.

CHAPTER TWO

LITERATURE REVIEW

2.1. Introduction

This section delves on the various literature resources reviewed on cloud computing and related issues. Herein, a logical connection is made of secondary information (includes white papers, journals, scholarly researched articles) from credible scholars of cloud computing. Our particular interest is on cloud computing, trust and adoption issues in higher education.

2.2. Cloud Computing

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 with 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 internet as opposed to hosting and operating those resources locally, such as on a college or university network." It depends on 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).

Advocates of cloud computing asserts that cloud computing makes it possible for organizations or institutions to avoid upfront infrastructure costs (Armburst et al., 2010) and focus on their core business (CSA, 2011; Anarudha & Janaka, 2014). Cloud computing also allows organisations to deploy their applications faster, with better manageability and less maintenance. This enables information technology to more rapidly align resources to meet changing and unpredictable business demand (Armburst et al., 2009). Higher education of learning can take this as an opportunity to increase IT agility to support areas of educational, research and innovation activities through cloud computing. Collaboration and mobility is also promoted through cloud computing (Durani & Bhatt, 2015).

2.2.1. Cloud Service Models

This is represented by 'SPI' Model which refers to 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; Mell & Grance, 2011) 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 allow 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.

2.2.2. 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).

2.2.3. Cloud Reference Model

The Cloud Security Alliance's cloud reference model (**Figure 2.0**) highlights the relationships and dependencies between the service models (SPI models).

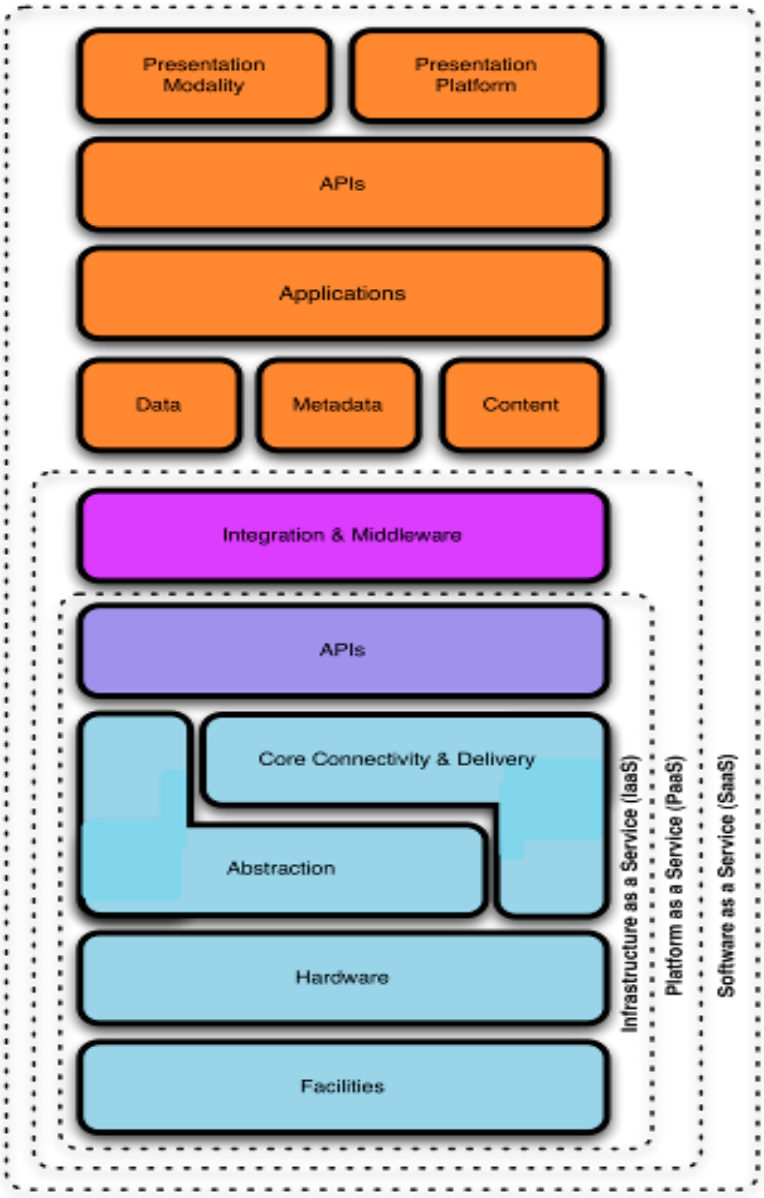


Figure 2.0 Cloud Reference Model (Source: CSA, 2009)

2.2.4. Traditional IT vs Cloud Computing

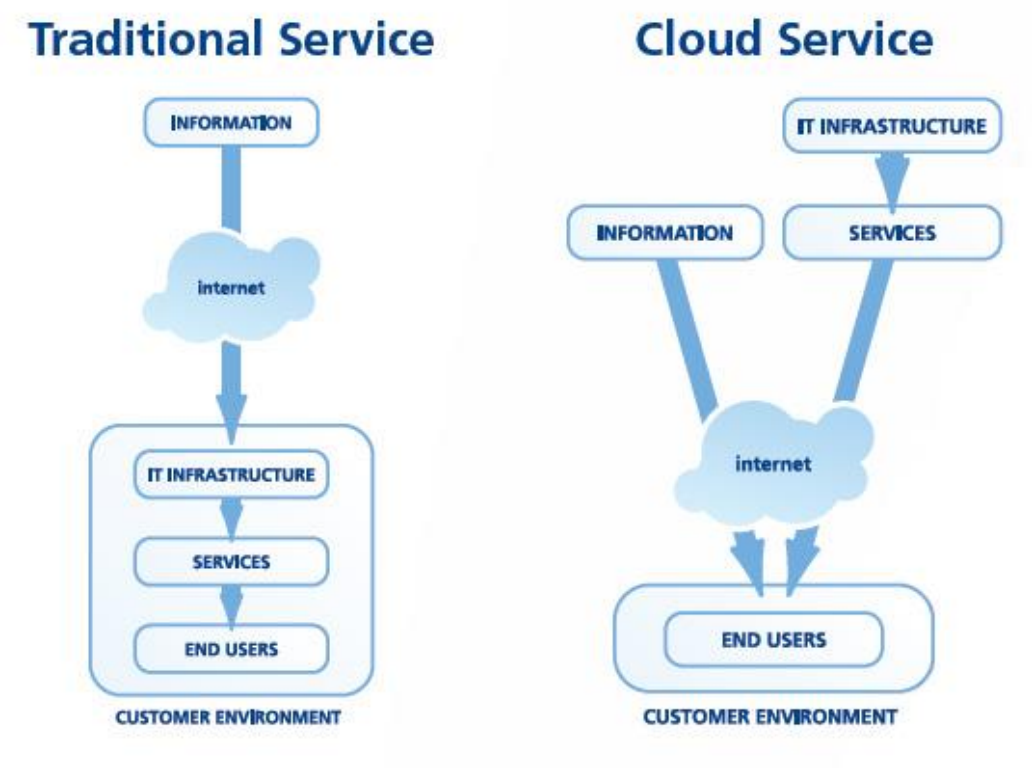


Figure 2.1 Traditional Service vs Cloud Service (Source: oem.stanford.edu)

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 service 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 & scholars) 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 better university curricula and expand research horizons for academic community using cloud computing model (Thomas, 2011)

The National Institute of Standards and Technology as indicated by Schyff & Krauss (2014) describes cloud computing five features as follows: broad network access, on-demand self-service, rapid elasticity and measured service, as well as resource pooling (CSA, 2011). On-demand self-service implies that a consumer is able to automatically assign services such as network storage to himself/herself without intervention from the service provider. Resource pooling means resources are assigned and issued based on demand through multi-tenant model. Measured service on the other hand implies metered services based on utilization. Resource usage is monitored and controlled; this promotes transparency for both user and service provider on resource utilization. Rapid elasticity offers the flexibility to scale outward or inward depending on service demand or requirement (CSA, 2011). Public cloud offers elasticity which is the ability to scale in or scale out. Through elasticity, the cloud client can be able to ask for additional services during high load or relinquishes the additional services at normal load (Marston et. al., 2011). This saves cost. However security cost associated with elasticity is high as well as there is concern over loss of control of data (Brown et. al., 2012). To the consumer, the provisioned services capability appears unlimited and hence is available in any quantity and can be given any time (Pearson & Benameur, 2010).

2.3. 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:

1. **Increased operational efficiency**

This improves IT agility and create more room for IT to be innovative. For the institution, 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.

2. **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:

- Ease of deployment of applications: running applications within a short time
- Flexibility: opens up opportunity for staff mobility; IT anywhere, anytime
- Sustainability: no need to invest in high calibre hardware, software or skilled resources
- Staff Redeployment: focus IT on high value tasks

2.4. 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:

- Security: 87.5%;
- Availability: 83.3%
- Performance: 82.9%.

From this research study, the key concerns of low adoption of cloud services in Kenyan Higher education by the key stakeholders in the education sector in regard to cloud computing will be identified.

2.5. 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 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 into cloud service providers' activities for companies whose data are on cloud or moving to cloud and they have very 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 health and financial sector, 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) defines trust as a situation where trustor is willing to depend on actions of trustee and therefore has no control of any actions or performance by 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.

Pearson & Benameur, (2010) posits that when evaluating trust in line with cloud computing, social and technological mechanisms should be taken as a way of presenting persistent and dynamic trust. They define persistent trust as long term and capable of supporting infrastructure while dynamic trust as short-term which emanates from context-based social and technological systems. Social-based trust and technological-based trust are deemed to relate through vouching mechanism, however, social-based trust is always taken into account as it determines the guarantor and what they are guaranteeing (Pearson & Benameur, 2010).

Cloud computing is also affected by perceived users view or perspective. Lack of control and transparency are some of the issues that affects users trust on cloud services which in effect has negative effect on cloud uptake rate (Khan & Malluhi, 2010). In distributed computing environment, trust is seen as having soft security elements which enforces its security mechanism. The security elements helps to fight against malicious entities thus enabling a cloud computing environment that is safe and secure (Chang, Sun & Wang, 2011; Minqi et. al., 2010).

2.5.1. 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).

2.5.2. 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.

2.5.3. Measuring Trust in Cloud

In trust relations, two entities are involved. One is the trustor and the other is the trustee. In cloud computing context, trustee provides required cloud services and trustor uses the services provided by the trustee. Huang and Nicol argues 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 highlights 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):

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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.

2.5.4. 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.

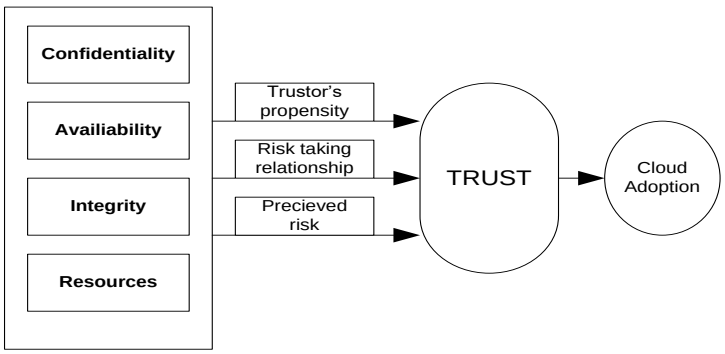


Figure 2.2 Conceptual Framework for Cloud Service (Source: Inspired by Mayers et al., 1995)

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

- 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.
- The trustor will exhibit some perceived risks that is bound to tests current trust. The outcome of the risk taking determines the uptake. This increases or decreases his or her level of trustworthiness, thus influencing adoption or subscribing to cloud services (Mayer et al.).
- 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. These will help us understand the varied views of key stakeholders that have an impact in cloud adoption or uptake.

2.6. Related Works:

Schyff & Krauss, (2014), carried out a research to understand trust and adoption issues affecting higher learning institutions in South African context. Their objective of study was to explore the views of key stakeholders with regard to cloud information security. This is carried out in three South African universities (two research intensive universities and a comprehensive university). A trust-centric framework is put forward in understanding and evaluating cloud computing adoption in Higher education context. The outcome of the research has shown that the purpose of a university does not necessarily allow for a generalization to be made; that trust in cloud security can be viewed as either internal or external to the university; it shows that stakeholders make judgments about whether cloud services can be trusted based on unfounded assumptions about cloud security and how cloud security is evaluated.

Mircea, et al. (2011) also conducted a research in higher institution of learning with a view of formulating a strategy to improve agility in the current financial crisis. The researcher's objective was to find alternatives to the use of IT, while leading universities to improve agility and obtain savings. The researcher's finding was that the economy was bound to force more organizations into adopting cloud solution. There were indications that universities had begun with the implementation and this was likely to decrease their expenses significantly.

Abdulsalam et al. (2011) conducted a research to explore the application of cloud computing in Higher education in Nigeria. The researcher looked at issues affecting ICT in Nigeria; touched on benefits and limitations of cloud computing. The outcome of research indicated that cloud computing may have considerable potential in improving ICT application and infrastructure in higher education institutions. Another outcome pointed out by the researcher is for the institutions to follow the hybrid approach where they will transition some application and data to cloud and leave others in house.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1. Introduction

This section is about the research methodology which was adopted for this study and which is influenced by the research aims and objectives. The methodology is founded on the analysis of the appropriate ways of answering the research questions and assessment of the collected data. The chapter is on the various research approaches seeking to address the research problem.

3.2. Research Design

The study employed the exploratory research design to collect critical information. With the exploratory design, various sources of information will be examined relating to the research problem. This is 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 research problem. Acknowledgement from journals, company reports, news articles of cloud computing, websites, IT Magazines, white paper and analysts report were referenced. The researcher is able to gain insight into the adverse factors of the research topic obtained through accurate secondary information (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 uptake by the key stakeholder in higher education. A set of universities were selected and requested to fill a questionnaire that was sent to the selected universities in five different counties in person. The dependent variable was usage 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. Wikipedia defines triangulation as a data validity technique through

cross verification from many sources. This also known as mixed approach employs qualitative research model to look into the stakeholder perceived assumption, behaviour and experience that is significant to the study and quantitative research model due to significant amount of data and feedback involved that will be significant to the study.

3.3. Target Population

The population of interest was drawn from an accredited list of both public and private chartered universities in Kenya. According to the Commission for University Education (Status of Universities Authorized to operate in Kenya 2013), there are 22 Public Chartered Universities and 17 Private Chartered Universities. Therefore, the total population was thirty nine (39) universities (without including the constituents' colleges).

3.4. Sample Design

Out of the 39 Universities (public and private chartered), a sample of 35% was selected, which translates to a number of 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. Systematic random sampling or interval sampling was applied in drawing samples for the research. This is one of the sampling techniques used in social science research (Mugenda, 2008). The sampling constant, K= N/n; where N in this study represents the Population and n represents the Sample size. This is shown as follows: K= 39/13=3

The first and every subsequent third university was selected from a list picked from information provided by the Commission for University Education on Status of Universities Authorized to operate in Kenya 2013 based on the date accredited (as attached in Appendix IV).

Target respondents for the study were systems administrators as they are the main implementers of the systems in place, IT Managers/Information Security Managers and other users of ICT.

3.5. Data Collection

Cohen, Manion & Morrison, (2007) states that the value of a research work and data collection techniques are linked to significantly involve both primary data 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 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. Other than the secondary data, primary data was collected from a sample of 4 from each thirteen (13) selected universities in Kenya. This gave a sample size of fifty two (52) questionnaires that were distributed.

The primary data collection technique used for this study was questionnaires. Creswell and Clark (2011) explains that a questionnaire allows for gathering of a large volume of information within a given time. A preliminary test of the research questionnaire was done specifically for clarity on research questions. We used Likert Scale questionnaire; the questionnaire was centred largely on availability, integrity, confidentiality and the resources capability. This was drawn from the conceptual framework. A pilot test was done involving some respondents who meet the sampling criteria. Following the pre-test, several areas requiring amendments were identified by the respondents and the researcher. These were amended by the researcher then it was validated. Validation of a questionnaire as pointed in Creswell and Clark (2011) ensures that questions are well founded and relate to the study (as shown in Table 3.1). The validated questionnaires were then shared in person to the selected universities to be issued to the targeted respondents.

Table 3.1: 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 will be phrased or directed to assess or measure resource capability of the institution.	This seeks to understand the institution 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 Kenya.	The questions under availability, integrity and confidentiality will guide in collecting the various views and fears of key decision makers in the selected institutions of higher learning.	This is to identify the main issues influencing the low uptake of cloud services in higher education of learning. This then will be useful in coming up with an adoption strategy or roadmap for increasing uptake of cloud computing in higher institutions of learning.

3.6. Data Analysis, Presentation and Interpretation

Data from secondary sources was analyzed based on the following criteria; one is the intended purpose of the reference source, like why it was written. Two is through assessment of the author's credentials in relation to the subject under consideration. The third criterion upon which secondary data has been analyzed is by looking at the source's data of publication as well as the intended audience for such material. The fourth criterion is on the subject coverage of the secondary source together with the appropriateness of its referencing (Sekaran & Bougie, 2010).

For primary data, the personal information gathered via the questionnaires was treated as confidential, and was part of the research results only. The unit of analysis was individuals in a university. The data gathered was analysed using SPSS and the results were presented in mean scores, percentages, illustrations, graphs and charts besides other statistical tools employed to present the findings. Subsequently, the collected primary data was compared with existing secondary information in the literature review section to provide a detailed response to the research question. On completion of the comparison, data validation and analysis, we were able to come up with the outcome results and recommendation for the study. This was to help in formulating the required framework for use as a guideline in implementing cloud computing in higher institutions for learning.

CHAPTER FOUR

DATA ANALYSIS AND INTERPRETATION

4.1 Introduction

This chapter presents the analysis, findings and discussions on usage of cloud computing in higher education: strategy to address trust issues in adoption of cloud services in Kenyan public and private universities. Survey questionnaires were administered to employees of the selected universities in Kenya that represented both the public and private universities. Selected employees were to respond on the usage of cloud computing based on availability, integrity, confidentiality and resources to manage the cloud computing services. The data was analyzed with the help of SPSS statistical package and presented using tables, charts, frequencies, percentages and some statistical summaries.

4.2 Background information and response rate

4.2.1 Response rate

The study involved fifty two (52) questionnaires which were issued to collect data from at least 4 employees of the thirteen (13) selected universities. Forty (40) questionnaires from ten universities were filled by the sampled employee and returned for analysis which gave 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 Kenyan public and private universities. According to Awino (2011), a response rate of 65 percent is acceptable for such studies and hence the response of this study was sufficient representation of the population within the universities as far as this study is concerned. The employee's response was captured in the table below as per their institution and department they serve. The respondents were to respond to questions on availability and reliability of infrastructures and productivity levels. They were also to respond on their resource skills capability, whether there are plans to adopt cloud computing and their current adoption level. They also responded on confidentiality and integrity of the policies for purchasing cloud computing resources by the universities in Kenya. The employees also ranked the cloud computing services and their efficiency for service delivery.

Table 4.1:Company/Institution * Section/Department Cross tabulation

Count

		Section/Department						Total
		Academics	Computer Science	ICT	IT	Multimedia	Network	
Company/Institution	Egerton	0	0	4	0	0	0	4
	GLUK	0	0	1	3	0	0	4
	KEMU	0	2	1	1	0	0	4
	MKU	0	0	4	0	0	0	4
	MMU	0	0	1	3	0	0	4
	PAC	2	0	2	0	0	0	4
	TUM	0	0	4	0	0	0	4
	UOE	0	0	4	0	0	0	4
	UON	0	0	2	0	0	2	4
	USIU	0	0	3	0	1	0	4
Total		2	2	26	7	1	2	40

From table 4.1., two of the respondents were from academics department, 2 were from computer science,7 were from IT, 1 was from multimedia department, 2 were from networking department and majority being 26 were from ICT department. This resulted to a total of 40 respondents as per the questions that were returned for analysis.

4.2.2 Personal Information on years of experience of respondents

The respondents were asked to provide information on their years of experience and they responded as in Table 4.2 below.

Table 4.2 Descriptive Statistics of 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					

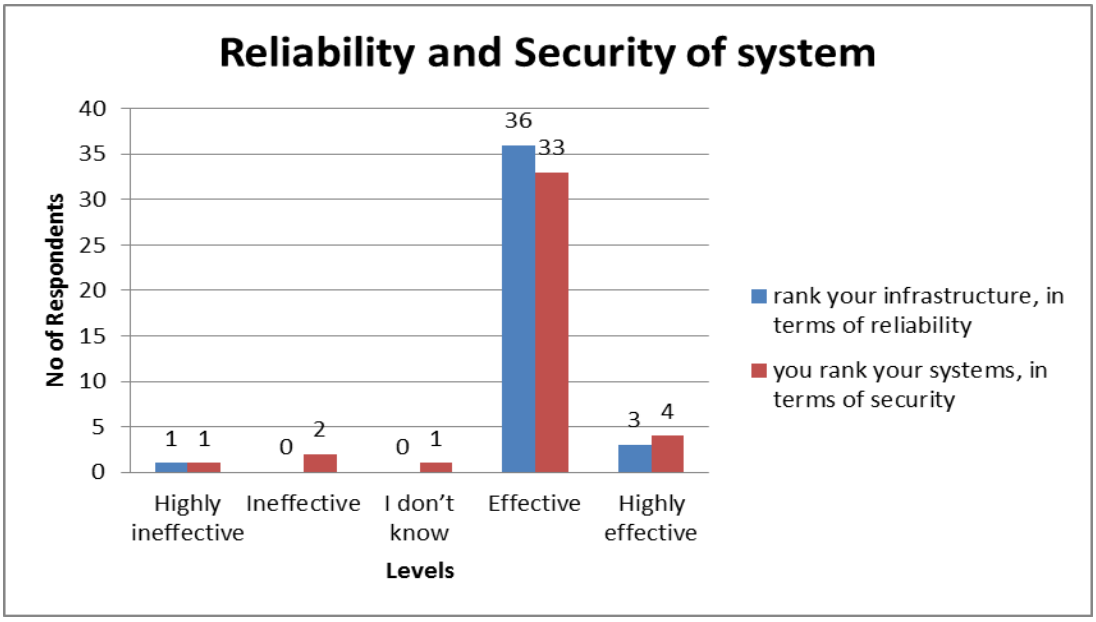
From Table 4.2, majority of the respondents had worked for an average of 5.17 years which portrayed their experience in their position of service in these institutions. Some employees had maximum experience of 14 years and some had minimum experience of 1 year. The standard deviation was small of 2.854 which indicates that majority of employees had almost same experience on average and this indicated that the employees had enough experience and hence they were in a position to give more reliable and valid information on usage of cloud computing in higher education in Kenya.

4.3Availability

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 were presented in the multiple bar charts below.

4.3.1 Availability and security of the system

Figure: 4.1 Bar-chart of Reliability and security of the systems.



From Figure 4.1, one of the respondents ranked both infrastructure in terms of reliability and system security as highly ineffective. Two of the respondents ranked ineffective their systems in terms of security, one did not know whether their system is secure. Majority of the respondents (36) ranked effective infrastructure availability in terms of reliability and 33 ranked effective systems 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.

4.3.2 Cloud services

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

Table 4.3 IaaS * any of your functions hosted on cloud Cross tabulation

Count

	any of your functions hosted on cloud					
	Strongly Agree	Somehow agree	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 service hosted on cloud, 13 somehow agreed, 1 was not sure, 4 somehow disagree and 8 strongly disagreed. Incidentally, only 4 respondents knows the type of cloud service model they are using. This indicates that some of the users do not know the type of cloud service model in use and some institution has not yet hosted any function on the cloud service. This means there is need for the technical staffs particularly 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.

4.3.3 Function Hosted on cloud

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

Table 4.4:Frequency table of functions hosted on cloud

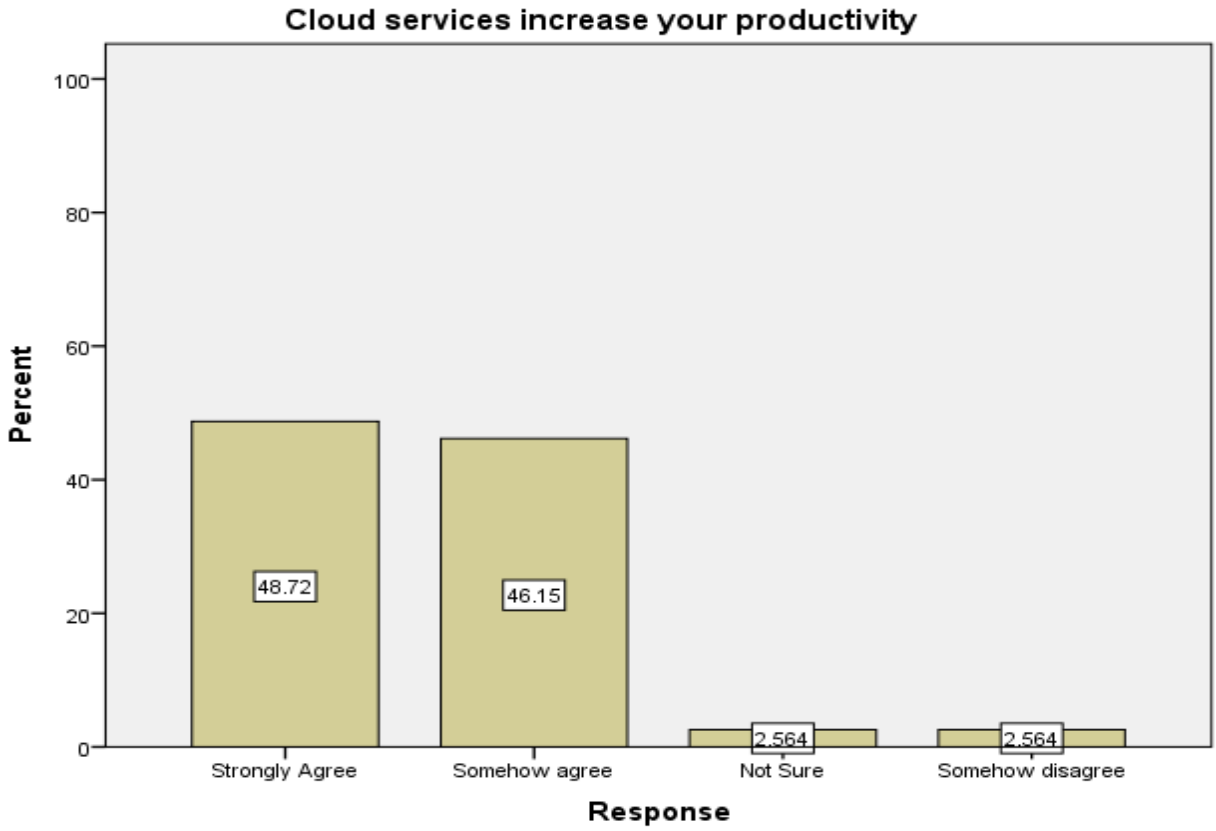
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	14	35.0	35.0	35.0
	Somehow agree	13	32.5	32.5	67.5
	Not Sure	1	2.5	2.5	70.0
	Somehow disagree	4	10.0	10.0	80.0
	Strongly disagree	8	20.0	20.0	100.0
	Total	40	100.0	100.0	

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 disagree and 20% strongly disagreed. This indicates that 67.5% cumulatively agreed that they host their services on cloud and it thus 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.

4.3.4 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: 4.2 Bar-chart of cloud services and productivity.



From Figure 4.2, 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 task leading to high operational efficiency. As a result, due to high available systems, this will increase staff performance leading to high productivity.

4.4 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 strategy that address trust issues in adoption

of cloud services in Kenyan public and private universities. The integrity in this study was discussion in the following sections:

4.4.1 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 4.5 Descriptive Statistics

	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 4.5, on rating of cloud services to any institution had a mean of 3.82 which is close to 4 and hence it's effective as per the Likert scale used. It had a very small 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 high confidence in cloud services it's something worth implementing. On if cloud services would lead to operational efficiency to their institution had a mean of 1.87 which is close to 2 and hence it's somehow agree as per the Likert scale used. It had a very small standard deviation of 1.056 which indicates that majority of the respondents had a common response of accepting that cloud services leads to operational efficiency. On if data hosted on cloud is secure had a mean of 2.37 which is close to 2 and hence it's somehow agreed as per the Likert scale used. It had a very

small standard deviation of 1.140 which indicates that majority of the respondents had a common response of accepting that data hosted on cloud is secure.

4.4.2 Stumbling blocks to cloud service adoption

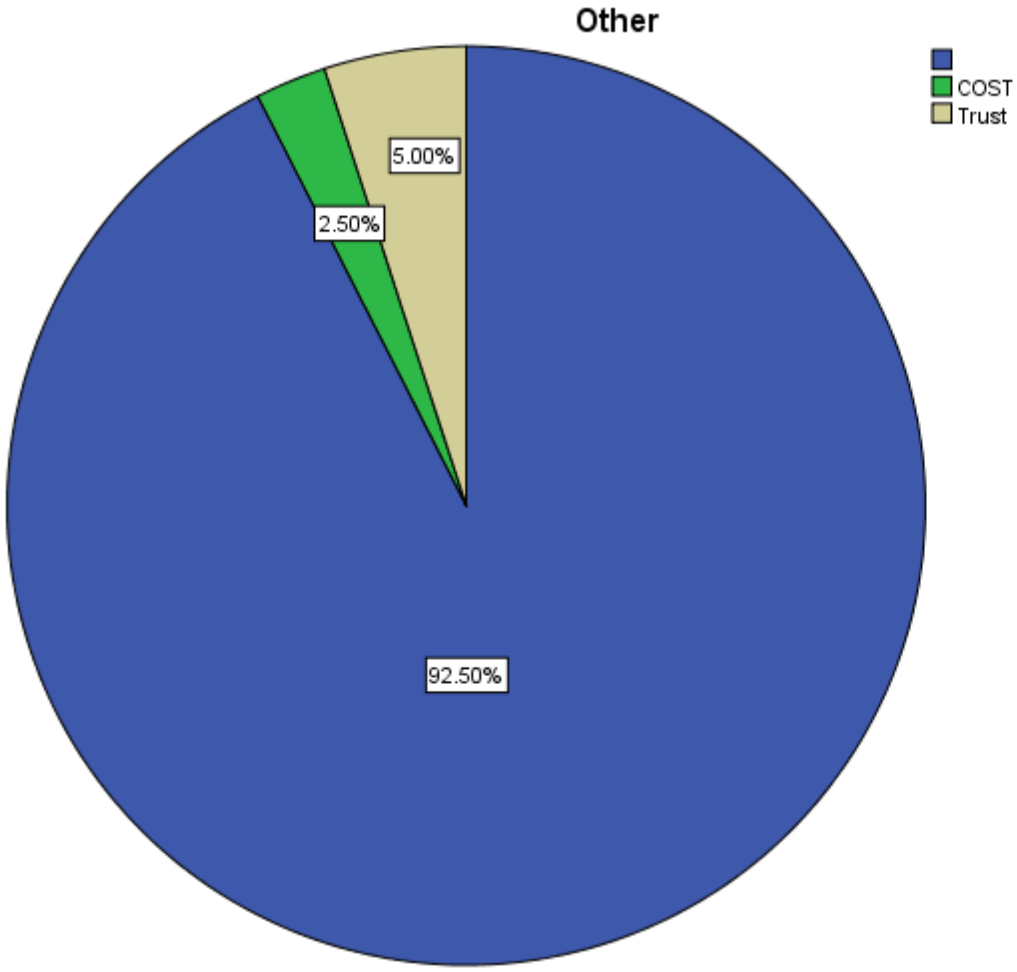
Table 4.6:One-Sample Test on stumbling blocks to cloud services adoption

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 4.6, Loss of control of data had a mean of 4.310 which is close to 4 and its high on Likert scale which indicates that loss of control of data is a stumbling block to cloud service adoption. Privacy had a mean of 4.194 which is close to 4 and it's high on Likert scale which indicates that Privacy is a stumbling block to cloud service adoption. Data Leakage / Loss had a mean of 3.613 which is close to 4 and it's high on Likert scale which indicates that Data Leakage / Loss is a stumbling block to cloud service adoption. Security had a mean of 4.071 which is close to 4 and it's high on Likert scale which indicates 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) which is highly and this means they all are stumbling block. Lack of standards and legal issues had (mean≤3.5) which is close to 3 and this moderate from Likert scale and hence it brings moderate stumbling block to cloud service adoption. 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 4.3 Pie-Chart for other stumbling blocks on cloud computing



From Figure 4.3, 2.5% indicated that cost was a stumbling block, 5.0% indicated that trust was a stumbling block to cloud services adoption. The rest who were majority did not suggest the other stumbling block.

4.4.3 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: 4.7 on capability and skills of service providers.

Cloud Service Provider capability and Skills

		Frequency	Percent	Cumulative Percent
Valid	Strongly Agree	9	22.5	22.5
	Somehow agree	21	52.5	75.0
	Not Sure	1	2.5	77.5
	Somehow disagree	3	7.5	85.0
	Strongly disagree	6	15	100.0
	Total	35	100	
Total		40	100.0	

From table 4.7, 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. For those who were not sure are 2.5%, somehow disagreed were 7.5% and 15% strongly disagreed. In general 75% of the respondents agreed that cloud service providers have the skills and capability to handle their institution 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 of the strategy should be to encourage information technology staffs within 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 uptake of cloud computing in higher learning institutions in Kenya.

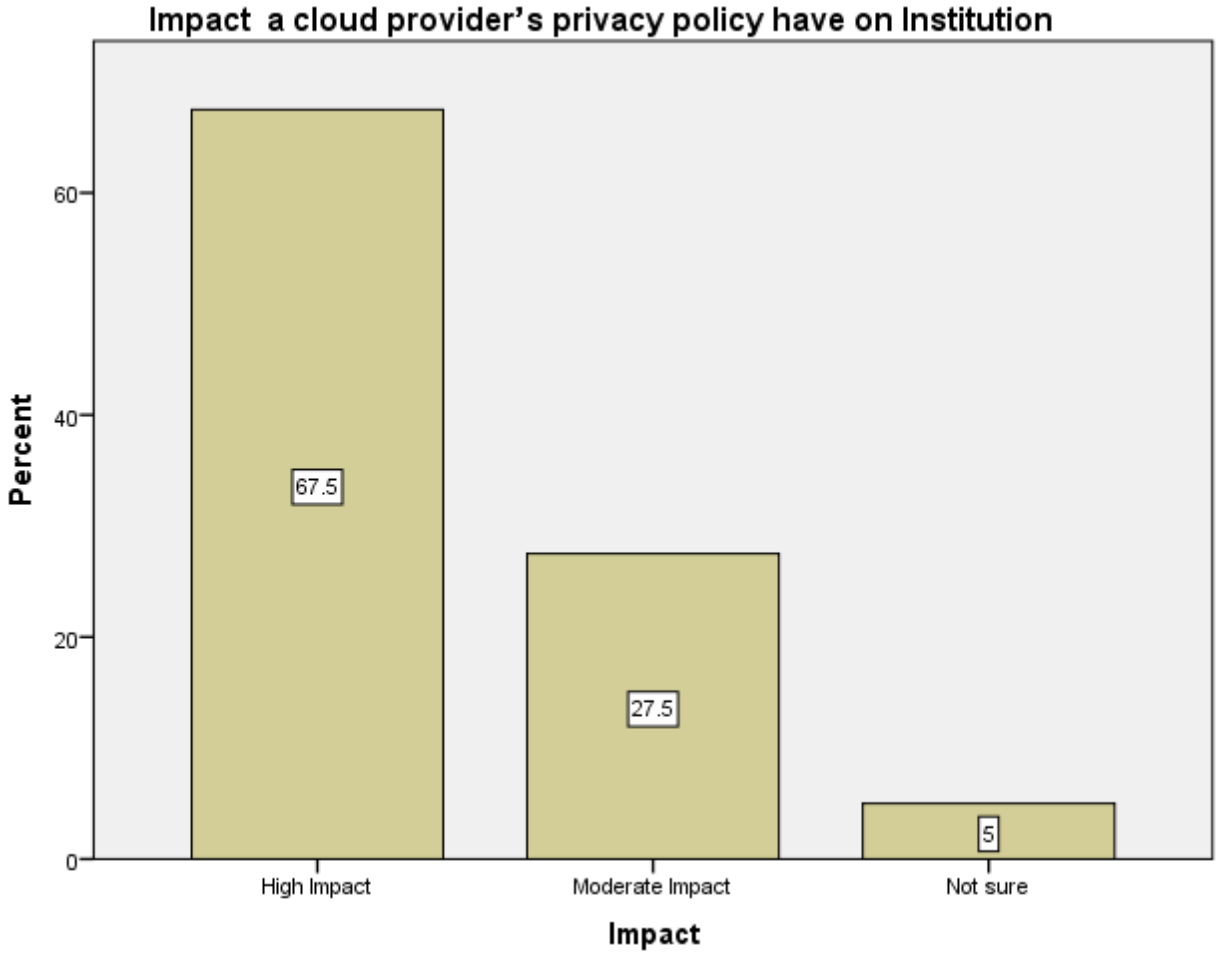
4.5. Confidentiality

In this section the respondents were asked on issues to do with the 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 Kenya. All these were discussed as follows.

4.5.1 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 respondent as in the figure below,

Figure 4.4 Bar-chart of the impact of cloud provider's privacy policy



From the Figure 4.4, majority of the respondents, 67.5% accepted that the impact is high on institutions cloud purchasing decision, 27.5% accepted that it had a moderate impact and 5% were not sure. From the study it indicates that about 95% indicates that the impact is there on cloud purchasing decision. This impact is a key barriers affecting adoption of cloud computing in Higher education in Kenya.

4.5.2 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 in the table below

Table 4.8 One-Sample Test of 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 4.8, Data Loss had a mean of 3.821 which is close to 4 and it's high on Likert scale which indicates 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 is close to 4 and it's high on Likert scale which indicates that un-availability of services & data has a high security threat rate which can hinder the adoption of cloud services. Privacy had a mean of 4.100 which is close to 4 and it's high on Likert scale which indicates that Privacy is a security threat to cloud computing and has high security threats which can hinder the adoption of cloud services. Shared technology vulnerability had a mean of

3.615 which is close to 4 and its high on Likert scale which indicates 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) which is high and this means they are security threats associated with cloud computing and have high security threats which can hinder the adoption of cloud services. Hypervisor vulnerability and legal issues had (mean≤3.5) which is close to 3 and this is moderate from Likert scale and theses are security threats associated with cloud computing and have moderate effect in hindering the adoption of cloud services. All their views on security threats associated with cloud computing had a significant value at p<.05 and this suggest that they had significant influence on adopting cloud services.

4.5.3 University handles /Respond to security threats.

The respondents were asked to give their views how their university handles /respond to security threats and they responded as in the table below

Table 4.9 Statistics on response to security

		Reporting incidences	Incidence Response Management	Threat Vulnerability Management	&Identity & Access Management
N	Valid	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 4.9, Reporting incidences had mode of 5 which is very frequently as per the Likert scale, this indicates that reporting incidences is very frequent way on how these institutions handle security threats. Incidence Response Management had mode of 4 which is frequently as per the Likert scale, this indicates Incidence Response Management is a frequent way on how these institutions handle security threats. Threat & Vulnerability Management had mode of 5 which is very frequently as per the Likert scale, this indicates threat & vulnerability management is a very frequent way on how these institutions handle security threats. Identity & Access Management had mode of 5 which is very frequently as per the Likert scale, this indicates identity & access management is a very frequent way on how these institutions handle security threats.

4.5.4 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 4.10 Statistics on 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 4.10, there is visibility over the cloud services being offered by the cloud service provider has a mean of 2.08 which is close to 2 which is somehow agree from Likert scale, 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 has a mean of 1.01 which is close to 1 which is strongly agree from Likert scale, this indicates that majority of the respondents strongly agree that there is need to hold accountable the cloud service providers based on the signed service level 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 service in their institutions.

4.6 Resources

In this section the respondents were asked on details to do with the resources within the higher learning institutions in Kenya. Their response was as indicated in the Table 4.11 below.

Table 4.11 Table on Resources

Resources	N	Mode	Std. deviation	Range
Have enough resources and skills to manage your systems in-house	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 4.11, have enough resources and skills to manage your systems in-house has a mode of 1 which is strongly agreed as per the Likert scale. Is their average working experience has a mode of 2 which is somehow agree as per the Likert scale and this indicates that majority of the respondents somehow agree that the institutions have average working experience.

Is cloud computing significant to your institution has a mode of 1 which is strongly agree as per the Likert scale and this indicates that majority of the respondents indicated that they strongly agree that cloud computing is significant to their institution. There are plans to adopt cloud computing fully as a cost cutting venture and to bolster operational efficiency in my institution has a mode of 2 which is somehow agree as per the Likert scale and this indicates that majority of the respondents somehow agree that institutions plans to adopt cloud computing fully as a cost cutting venture and to bolster operational efficiency in their institution. What Stage is your institution in with regard to cloud services adoption has a mode of 1 which is already in use/implementing as per the Likert scale and this indicates that majority of the respondents agreed that their institutions were already in use/implementing with regard to cloud adoption.

4.7 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 4.12 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. Hence, this enables the questionnaire to be more reliable for the study.

4.8 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 4.13) and regression analysis as a comparison (Table 4.14).

Table 4.13 One-Sample Test of Independent variables

	Test Value = 0					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Resources	21.692	39	.000	1.892	1.72	2.07
availability2	41.081	39	.000	3.019	2.87	3.17
Confidentiality2	33.744	39	.000	3.202	3.01	3.39
Integrity2	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 have significance influence on the adoption of cloud computing in the institution of higher learning in Kenya.

Table 4.14 Regression analysis table on effects of dependent and independent factors

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(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 is 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 have positive effects while confidentiality have a negative effect on adoption of cloud computing in universities in Kenya.

4.9 Cloud Adoption Strategy for Higher Education of Learning

A well- defined cloud adoption strategy must align to the institutions overall strategy as well as IT strategy for maximum reaping of the cloud computing benefits. We propose a 5 stages roadmap strategy to be adopted in Higher education of learning in Kenya to address the cloud adoption uptake issue

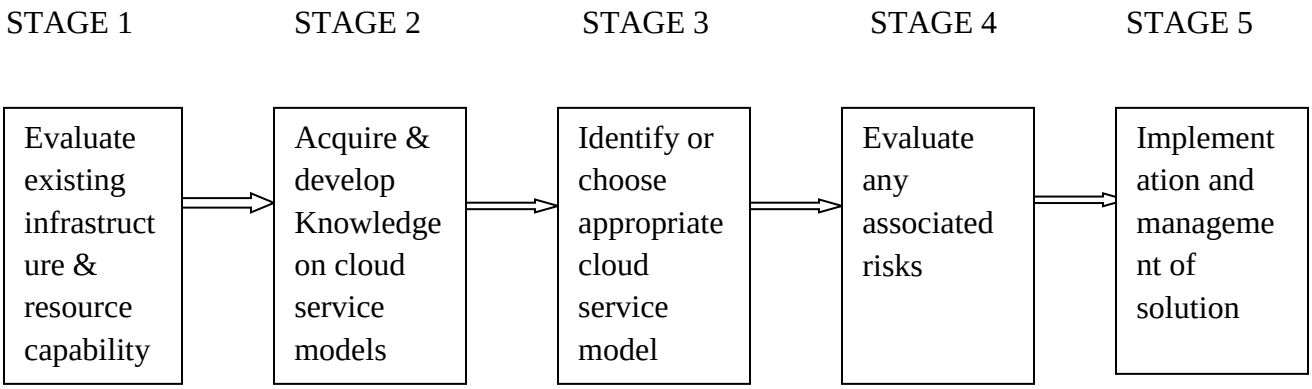


Figure 4.5 Roadmap Strategy to be adopted

Stage 1

Stage one involves an assessment of the institutions infrastructure capability as well as the resource capability. SWOT matrix tool may be used to assess the strengths and weaknesses as well as the opportunities and threats of the existing infrastructural systems and the resource capabilities. Policies and standards should also be reviewed under this stage.

Stage 2

This stage involves gathering and developing knowledge about the various types of cloud models. The information technology personnel in institution of learning can be sponsored by their institutions to attend seminars, conferences, workshops on cloud computing solutions so that they can acquire substantial knowledge on cloud computing. Also through cloud service providers' engagement, they can get to learn on new cloud solutions in the market. Benchmarking also assist in getting to know some of the best practices applicable with cloud solutions. Knowledge base repository is ideal for storing and sharing this information.

Stage 3

Under this stage, performing a cost benefit analysis is essential. Business case highlighting the benefits associated with the selected solution and budgetary requirements is ideal. Involvement of key stakeholders or decision makers at this level is important as it keeps them in the know of the capital required for initial test plan and complete implementation of the solution. Depending on the model selected, the institution can identify the priority applications that will require to be hosted on cloud. Hence, a migration plan will be required to be in place.

Stage 4

Risk Evaluation is important as it enables the cloud consumer assess the potential or service provider capability. At this stage, evaluation of legal, contractual and compliance issue is pertinent. It's also important to carry out an audit of the cloud service provider's facility besides the SLA (Service Level Agreement) document provided to ensure integrity, confidentiality and availability is clearly addressed. Cloud provider privacy policy should also be analyzed critically to assess any data exposure risk. Relevant and specific metrics should be provided in the SLA for monitoring purpose.

Stage 5

The last stage is the implementation and management of the solution after successful deployment. Documentation of the processes involved is important for the team supporting the solution. Training of IT staff is necessary to act as first level support in-house. Feedback mechanisms is part of the stage to test effectiveness. Cloud services or solutions if successfully implemented will help in cost cutting as it will be easy to deploy applications quickly without being worried of hardware or software cost. This lowers the CAPEX and increases scalability of the systems in place. The other benefit that will be seen is increased IT agility and flexibility to concentrate on innovation as opposed to problem solving.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the conclusions drawn from the findings highlighted in Chapter four and recommendations made there-to. The conclusions and recommendations drawn were focused on addressing the objectives of this study which were to find alternative to use of IT through cloud, while leading higher institutions of learning to increase operational efficiency and cut cost, Identify key barriers affecting adoption of cloud computing in Higher education in Kenya, and develop a strategy or roadmap for adoption of cloud computing in Higher Education in Kenya.

5.2 Conclusions

The following conclusion was reached following the analysis of the statistical data collected from the respondents. Our conclusion seeks to address the 3 objectives of the study.

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

   From the first objective, the following conclusions were reached:

   The study concludes that there is a growing receptiveness of cloud computing services in the institution of higher learning. 67.5% hosts services on cloud but only 10% knows what the type of cloud model is in use by their institution. Infrastructure as a Service (IaaS) is the cloud model used by these institutions. This means that there is need for these institutions to ensure their information technology team are well versed 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 deployments. 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 close to 4 on the Likert Scale denoting "effective". Majority of the respondents also indicated that data hosted on cloud is secure; this had a mean score of 2 meaning "effective" on the Likert Scale.

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 service increases productivity. This means that cloud services will aid in enhancing performances of the 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 "Identify key barriers affecting adoption of cloud computing in Higher education in Kenya."**

   From the second objective, we make the following conclusions guided by the statistical analysis of the respondents view:

   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 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; hence, further study needs to be done to ascertain the extent cost and trust plays as a factor in 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 provisioned 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 to increased uptake of cloud services. 95% of the respondents cumulatively 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 Kenya."**

   All objectives were met resulting to a formulation of a 5 stage strategy to be used by higher education 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.

5.4 Recommendation from the study geared towards increasing cloud uptake in institutions of Higher Learning in Kenya

The implications of the findings for this study for practice are these. First, to promote cloud computing among institution of learning, cloud service providers should be transparent with their privacy policy in their engagements with the institutions as this has a high impact on cloud purchasing decisions in these institutions. Second, there is need for training and creating cloud services awareness (through workshops, benchmarking and seminars) in the institution of learning to increase adoptability by the key stakeholders. Third, alignment of IT strategy and cloud adoption strategy to the institution's corporate strategy is key.

5.5 Limitations of the Study

The study was completed and reached its aim despite the following limitations:

1. Not all respondents managed to respond to the questionnaire. This however did not deter the study in any way as a response rate of 76.9% was a good representation of the general population.
2. Limitation in monetary resources and time did affect collection of data and analysis since it involved a lot of travel. To mitigate this, we resorted to use of email as another mode of sharing the questionnaire with the respondents. As a result, this made the data analysis to

take longer as we had to consistently follow up with the respondents to provide their feedback on the questionnaire.

5.6 Recommendations for Further Research

Future studies should focus on the following areas to ensure these institutions operate effectively:

I. Study on implementation challenges while adopting cloud services in higher education.

II. Study on cost and trust as stumbling blocks and how they affects cloud adoption in higher education.

III. Study on the effective ways of implementing the roadmap to increase cloud computing in Higher Education in Kenya

REFERENCES

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.

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

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*.

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, 2011.

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

Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf, Recommendations of the National Institute of Standards and Technology; *NIST Cloud Computing Reference Architecture.*

https://cloudsecurityalliance.org/group/cloudtrust/Strategy&, Formerly Booz & Company; Cloud computing, "*An information security perspective*";

http://www.strategyand.pwc.com/media/file/Strategyand_Cloud-computing.pdf

R.C. Mayer, J.H. Davis, and F.D. Schoorman, "An Integrative Model of Organizational Trust," Academy of Management Review, *Vol. 20, 1995, p. 709-734.*

Becky J. Starnes, Stephen A. Truhon, Vikkie McCarthy; Organizational Trust: *Employee-Employer Relationships.*

Huang and Nicol Journal of Cloud Computing: Advances, Systems and Applications 2013, 2:9; *http://www.journalofcloudcomputing.com/content/2/1/9*

Challenges of implementing e-learning in Kenya: A case of Kenyan public universities John K. Tarus, David Gichoya, Alex Muumbo

Cartes Secure Connexions, Cloud computing press release October, 2014; "Towards Secure Cloud Use."

http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909616

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

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.*

EDUCAUSE, "7 things you should know about cloud computing.'' *https://library.educause.edu/~/media/files/library/2009/8/est0902-pdf.pdf*

Thomas, P. Y. (2011). Cloud computing: a potential paradigm for practicing the scholarship of

teaching and learning. *The Electronic Library*, 29 (2): pp. 214-224.\

Cisco. White paper: Cloud Computing in Higher Education: A Guide to Evaluation and Adoption. https://www.cisco.com/web/offer/email/43468/5/Cloud_Computing_in_Higher_Education.pdf

White Paper: Identity and Access Management for Approaching Clouds

http://www.ca.com/us/~/media/files/industryanalystreports/cloud_security_wp_236234.aspx

E.O Makori: "Cloud Computing Paradigm and Libraries and Information Establishments in Kenya: *Any Opportunities for Operational Resilience*?"

http://uk.idc.com/downloads/security_briefing_pres.pdf

https://www.eiseverywhere.com/file_uploads/86cde4f4bf015bb8cd2153ea7e0287ff_Day_1_815am_Frank_Gens_Bringing_Cloud_into_the_Enterprise.pdf

G. Reese, Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, in: *Theory in Practice, O'Reilly Media, 2009*

Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou "Security and Privacy in Cloud Computing: *A Survey" in IEEE 2010*.

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*

Ryan, P. and Falvey, S. (2012). Trust in the clouds. Computer Law and Security Reviews, 28, *513-521. http://dx.doi.org/10.1016/j.clsr.2012.07.002*

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*

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

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. doi:10.1016/j.future.2012.01.006*

Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, *16, 108-114.doi:10.1016/j.istr.2011.08.006*

Zissis, D and Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28, 583–592. doi:10.1016/j.future.2010.12.006*

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. NIST Special *Publication 800-145, September 2011*

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

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011).Cloud computing — The business perspective. Decision Support Systems, 51, 176–189. *doi:10.1016/j.dss.2010.12.006*

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

W. J. Brown, V. Anderson, and Q. Tan, "Multitenancy-security risks and countermeasures," in Proceedings of 2012 15th International Conference on Network-Based Information Systems (NBiS), *Melbourne, Australia, 2012, pp. 7-13*

Pathan A.-S.K., Mohammed M.M.Z.E, (2015) "Building Customer Trust in Cloud Computing with ICT-Enabled Regulatory Body".

WANG, C.; REN, K.; LOU, W. & LI, J. (2010): Toward publicly auditable secure cloud data storage services. Network, IEEE, vol. 24, 19-24. *http://dx.doi.org/10.1109/MNET.2010.5510914*

Cloud Security Alliance, (2011). "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0". *http://www.cloudsecurityalliance.org/guidance/csaguide V3.0.pdf*

Teneyuca, D. (2011). Internet cloud security: The illusion of inclusion. Information Security Technical Report, *16, 102-107. doi:10.1016/j.istr.2011.08.005*

Murdoch, N. (2010): "The White Choice: Should you Head into the Cloud?" Proctor 24: 24

Cisco (2011) white paper: Cloud Computing Advantages in the Public Sector.

Durani, H & Bhatt, N (2015), “Cloud Computing in Higher Education: Gujarat State

N Vijaykumar, “Role of ICT in e-governance: Impact of Cloud Computing in Driving New initiatives”, *SETLABS Briefings, Vol9 No2, 2011*

YOO, C. S. (2011): "Cloud computing: Architectural and policy implications," *Review of Industrial Organization, vol. 38: 405-421*

Appendix I: Questionnaire

SECTION A: Personal information

1. Name (optional) ……
2. Company (optional)……..
3. Position……..
4. Number of years' experience in the current position (whether in current organization or from another organization ……..
5. Section/Department…….

SECTION B:

A: AVAILABILITY

1). How would you rank your infrastructure, in terms of reliability?

(1) Highly ineffective ☐ (2) Ineffective ☐ (3) I don't know ☐

(4)Effective ☐ (5) Highly effective ☐

2). How would you rank your systems, in terms of security?

(1) Highly ineffective ☐ (2) Ineffective ☐ (3) I don't know ☐

(4) Effective ☐ (5) Highly effective ☐

3). Are any of your functions hosted on cloud?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

4). i. If Yes (on above question), what type of Cloud service?

(1) IaaS ☐ (2) PaaS ☐ (3) SaaS ☐ (4) I don't know ☐

ii. Name the functions….

5). In your view, would cloud services increase your productivity?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

B: INTEGRITY

6). How would you rate cloud services to any organization?

(1) Highly ineffective ☐ (2) Ineffective ☐ (3) I don't know ☐ (4) Effective ☐ (5) Highly effective ☐

7). In your view, would cloud services leads to operational efficiency?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

8). In your opinion, is data hosted on cloud secure?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

9). In your opinion, what do you think is a stumbling block to cloud services adoption?

☐ Loss of control of data

☐ Privacy

☐ Data Leakage / Loss

☐ Transparency

☐ Security

☐ Compliance Issues

☐ Contractual Issues

☐ Availability

☐ Performance

☐ Data Portability / migration Issue

☐ Others (Please Specify)……

10). In your view, would you consider Cloud Service Provider as having the capability and skills to handle any of your institution data?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

C: CONFIDENTIALITY

11). In your opinion, what impact would a cloud provider's privacy policy have on your institution cloud purchasing decision?

1) High impact ☐ (2) Moderate impact ☐ (3) Low impact ☐

(4) No impact ☐ (5) Not sure ☐

12). In view of all the benefits associated with cloud computing, what security threats will hinder you from adopting cloud services?

☐ Data Loss

☐ Availability of services & data

☐ Privacy

☐ Shared technology vulnerability

☐ Security (application security, controls)

☐ Vendor Lock-in

☐ Hypervisor vulnerability

☐ Insecure API's

☐ Others (Please Specify)……

13). How does your university handle or respond to security threats?

- ☐ Reporting incidences
- ☐ Incidence Response Management
- ☐ Threat & Vulnerability Management
- ☐ Identity & Access Management
- ☐ Others (Please Specify)……

14). There is visibility over the cloud services being offered by the cloud service provider.

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

15). There is need to hold service providers accountable based on the service level agreement signed.

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

16). Transparency of the cloud service operations might influence the cloud adoption process within the institution.

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

D: RESOURCES

17). Do you have enough resources and skills to manage your systems in-house?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

18). What is their average working experience?

1) Less than 5 Years ☐ (2) 5 - 10 Years ☐ (3) 11 – 15 Years ☐

(4) Over 15 Years ☐

19). In your opinion, is cloud computing significant to your institution?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

20). There are plans to adopt cloud computing fully as a cost cutting venture and to bolster operational efficiency in my institution.

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

21). What stage is your institution in with regard to cloud services adoption?

1) Already in use / Implementing ☐ (2) Evaluating cloud for specific needs ☐

(3) Planning to adopt in 1-2 Years ☐ (4) Learning about cloud ☐

(5) No plans for cloud ☐

Appendix II: Revised Questionnaire (Set 2)

SECTION A: Personal information

1. Name (optional) ……
2. Company/Institution ……..
3. Position……..
4. Number of years' experience in the current position (whether in current organization or from another organization ……..
5. Section/Department…….

SECTION B:

A: AVAILABILITY

1). How would you rank your ICT infrastructure, in terms of reliability?

(1) Highly ineffective ☐ (2) Ineffective ☐ (3) I don't know ☐

(4)Effective ☐ (5) Highly effective ☐

2). How would you rank your ICT systems, in terms of security?

(1) Highly ineffective ☐ (2) Ineffective ☐ (3) I don't know ☐

(4) Effective ☐ (5) Highly effective ☐

3). Are any of your functions hosted on cloud?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

4). i). If Yes (on above question), what type of Cloud service?

(1) IaaS ☐ (2) PaaS ☐ (3) SaaS ☐ (4) I don't know ☐

ii). Name the functions……..

5). In your view, would cloud services increase your productivity?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

B: INTEGRITY

6). How would you rate cloud services to any organization?

(1) Highly ineffective ☐ (2) Ineffective ☐ (3) I don't know ☐ (4)Effective ☐
(5)Highly effective ☐

7). In your view, would cloud services leads to operational efficiency?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

8). In your opinion, is data hosted on cloud secure?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

9). To what extent do the following obstacles influence cloud services adoption in your institution?

Obstacle	Very Highly (5)	Highly (4)	Moderately (3)	Low (2)	I don't Know (1)
Cost					
Loss of Control					
Infrastructure					
Transparency					

Compliance					
Security					
Performance					
Availability					
Data Portability/Migration Issue					
Lack of standards					
Legal issues					
Others (Please specify)…….					

10). In your view, would you consider Cloud Service Provider as having the capability and skills to handle any of your institution data?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

C: CONFIDENTIALITY

11). In your opinion, what impact would a cloud provider's privacy policy have on your institution cloud purchasing decision?

1) High impact ☐ (2) Moderate impact ☐ (3) Low impact ☐

(4) No impact ☐ (5) Not sure ☐

12). To what extent do the following security threats hinder you from adopting cloud services in your institution?

Threats	Never (1)	Rarely (2)	Moderately (3)	Highly (4)	Very Highly (5)
Data Loss					
Services or data un-availability					
Privacy					
Shared technology vulnerability					
Application Control					
Vendor Lock -in					
Hypervisor Vulnerability					
Insecure API					
Others (Please Specify)……..					

13). Indicate the extent to which the following apply, as an approach to handle or respond to security threats in your institution.

Approach	Very Frequently (5)	Frequently (4)	Sometimes (3)	Rarely (2)	Never (1)
Report Incidences					
Incidence Response Management					

Threat & Vulnerability Management					
Identity & Access Management					
Others (Please specify)…….					

14). There is visibility over the cloud services being offered by the cloud service provider.

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

15). There is need to hold service providers accountable based on the service level agreement signed.

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

16). Transparency of the cloud service operations might influence the cloud adoption process within the institution.

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

D: RESOURCES

17). Do you have enough resources and skills to manage your systems in-house?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

18). What is their average working experience?

1) Less than 5 Years ☐ (2) 5 - 10 Years ☐ (3) 11 – 15 Years ☐

(4) Over 15 Years ☐

19). In your opinion, is cloud computing significant to your institution?

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

20). There are plans to adopt cloud computing fully as a cost cutting venture and to bolster operational efficiency in my institution.

1) Strongly Agree ☐ (2) Somehow agree ☐ (3) Not Sure ☐

(4) Somehow disagree ☐ (5) Strongly disagree ☐

21). What stage is your institution in with regard to cloud services adoption?

1) Already in use / Implementing ☐ (2) Evaluating cloud for specific needs ☐

(3) Planning to adopt in 1-2 Years ☐ (4) Learning about cloud ☐

(5) No plans for cloud ☐

Appendix III: Letter of Introduction

Daniel Ochieng Onyango
School of Computing and Informatics
University of Nairobi

March 1, 2016

Dear Respondent,

I am pursuing a Master's degree in Information Technology Management at University of Nairobi. In partial fulfilment of the requirements for the award of degree of Master's in Information Technology Management, I am conducting a study entitled, "Using Cloud Computing in Higher Education: A Strategy to Address Trust Issues in Adoption of cloud services in Kenyan Public and Private Universities."

To be able to carry out this study successfully, you have been picked to form part of the study. I kindly request for your assistance in filling the attached questionnaire which forms part of collecting required data for the study. All information will be treated with utmost confidentiality and used for academic purpose only.

Thank you in advance for your assistance.

Yours faithfully,

Daniel Ochieng Onyango — **MSC Student**

Professor Elijah Omwenga — **MSC Project Supervisor**

Appendix IV: Public & Private Chartered Universities in Kenya

University (Public & Private) in Kenya	Date accredited
University of Nairobi	1970
Moi University	1984
Kenyatta University	1985
Egerton University	1987
University of Eastern Africa, Baraton	1991
Catholic University of East Africa	1992
Jomo Kenyatta University of Technology	1994
Daystar University	1994
Scott Christian University	1997
United States international University	1999
Maseno University	2001
African Nazarene University	2002
Kenya Methodist University	2006
Masinde Muliro University of Science and Technology	2007
St. Paul university	2007
Pan Africa Christian University	2008
Strathmore University	2008
Kabarak University	2008
Mount Kenya University	2011

Africa International University	2011
Kenya Highlands Evangelical University	2011
Great Lakes University of Kisumu	2012
Dedan Kimathi University of Technology	2012
KCA University	2013
Adventist University of Africa	2013
Chuka University	2013
Technical University of Kenya	2013
Technical University of Mombasa	2013
Pwani University	2013
Kisii University	2013
University of Eldoret	2013
Maasai Mara University	2013
Jaramogi Oginga Odinga University of Science and Technology	2013
Laikipia University	2013
South Eastern Kenya University	2013
Meru University of Science and Technology	2013
Multimedia University of Kenya	2013
University of Kabianga	2013
Karatina University	2013