A SECURE CLOUD-BASED ACADEMIC ENTERPRISE RESOURCES PLANNING (CAERP) MODEL FOR HIGHER INSTITUTIONS

"A CASE STUDY OF KAMPALA INTERNATIONAL UNIVERSITY, UGANDA"

BY

IBRAHIM ADABARA

1165-04256-10227

OCTOBER 2019

A SECURE CLOUD-BASED ACADEMIC ENTERPRISE RESOURCES PLANNING (CAERP) MODEL FOR HIGHER INSTITUTIONS

"A CASE STUDY OF KAMPALA INTERNATIONAL UNIVERSITY, UGANDA"

Master`s Degree Dissertation Submitted to the

Directorate of Higher Degrees and Research

Kampala International University

Kampala Uganda

In partial fulfillment of the requirements for the degree of

Master of Science in Information Technology

By

IBRAHIM ADABARA

1165-04256-10227

OCTOBER 2019

DECLARATION

Student declaration:

I hereby declare that this submission is my work towards Masters of Science in Information Technology and that to the best of my knowledge, it contains no material previously published by another person or material which has been accepted for the award of any other degree of the University, except where due acknowledgement/reference has been made to the work.

Signature: …… Date: ……...

IBRAHIM ADABARA

1165-04256-10227

ACKNOWLEDGEMENT

I am grateful to God for bringing me this far in this study. Its profound gratitude goes to my supervisor Dr. Sanni Shamsudeen, the Dean, Dr. Kareyo Margaret, Prof. Gonzalez Vincent (Chairman, Postgraduate Seminar Committee), and the Head of Department, Information Technology; Mr. Asiimwe J. Patrick for their tireless professional guidance, directions, advice, and contributions. I would like to appreciate other staff members who have contributed to my academic career one way or the other, especially Dr. Ajiboye Adeleke Raheem, Dr. Yakubu A., Dr. Chinecherem Umezuruike, Dr. Olutola Fagholu, and Dr. Malinga Ramadhan, Thank you very much, sir and madam.

I am indebted to my family, most notably my lovely wife, Mrs. Adabara Efe Margaret, for her timeless prayers and support in every ramification. My wonderful son (Adabara Harrison Adesire), thank you so much for your patience and prayers. My ever-loving late parents, I will forever miss and be grateful for all you taught me.

I will also like to express my sincere appreciation to all my colleagues in the School of Engineering and Applied Sciences Dr. Atiku M, Dr. Lawal O, Eng. Ajiboye Priscilla .O. Mr. Mundu M., Mr. Lasisi Kamoru, and Mr. Oyagbola Ismail, for all the timely encouragement. I am very grateful.

APPROVAL

I affirm that the work presented in this thesis was carried out by the candidate under my supervision.

Signature …… Date ……

Dr. Sanni Shamsudeen

Supervisor

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

APIs	Application Program Interfaces
AWS	Amazon Web Services
BPaaS	Business Process as a Service
CapEx	Capital Expenditures
CERP	Cloud-based Enterprise Resource Planning
CCAUM	Cloud Computing Adoption and Use Model
CC	Cloud Computing
CDs	Compact Discs
CSF	Critical Success Factors
DaaS	Data storage as a Service
DBaaS	Database as a Service
EC2	Elastic Compute
ERP	Enterprise Resource Planning
HaaS	Hardware as a Service
IaaS	Infrastructure as a Service
IBM	International Business Machines
ICT	Information Communication Technology
IPMaaS	Identity and Policy Management as a Service
IT	Information Technology
KIU	Kampala International University

MWaaS	Middleware as a Service
NaaS	Network as a Service
OpEx	Operating expenses
PDAs	Personal Digital Assistants
PaaS	Platform as a Service
REST	Representational State Transfer
S2aaS	Sensing as a Service
S3	Amazon Simple Storage Service
SaaS	Software as a Service
SLAs	Service-Level Agreements
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
TCO	Total Cost of Ownership
VCL	Virtual Computing Lab
VM	Virtual Machine
VPN	Virtual Private Network
XML	Extensible Markup Language

ABSTRACT

Academic Enterprise Resource Planning (ERP) systems are meant to integrate the separate activities, processes, and functions within a higher institution to help streamline the process and to provide real-time, on-demand information needs. The volume of data produced by academic institutions grows every day. Due to the increasing numbers of staff, students, departments, and programs, this continuous growth requires continuous scaling and improvement of the academic ERP system. Therefore, to adapt to this continuous growth, the system should be constructed based on a cloud computing platform. Cloud-based Enterprise Resource Planning system address many security and privacy issues in higher institutions: the increase of data/information, cost of hardware/software, data alteration, loss of data during migration from one server to another server, limited teaching materials and resources, high administrative costs, difficulties in managing large population of learners against small number of lecturers. This study designed a security and privacy model for an academic cloud-based ERP system. In this study, the researcher used a qualitative research design to examine the current server-based ERP system for Kampala International University and descriptive design to determine the requirements for the development of a secure model for cloud-based ERP system, which was guided by a well-structured interview guide and expert panel. Data was collected from the ICT department, interviewing four staff who manage the current server-based ERP system. The findings from this study showed that higher institution is faced with security and privacy challenges that compromise the Confidentiality, Integrity, and Availability of data/information. Also, a security and privacy model was developed, which was guided by the findings from the analysis of the face to face interview, the expert panel conducted as well as literature reviewed. It is recommended that higher institution should migrate to cloud computing, Infrastructure as a Service (IaaS) should be adopted since higher institution are concerned with security and privacy issues in the cloud, Data Encryption and Tokenization should be used when storing data/information in the cloud and also comply with the ISO27002 security standard after migrating to the cloud. Hence, it is undeniable that a cloud-based ERP system provides a secure environment, reduces costs in terms of hardware, software, upgrades, up-front expenses, and promotes mobile computing, which is the ability to access resources from anyplace at any time.

Keywords: Cloud Computing, ERP, Higher Institution, Privacy, and Security.

CHAPTER ONE

INTRODUCTION

1.0 General introduction

It is a known reality that Higher Institutions of learning play a significant role in the growth of societies. Alharthi et al. (2015). Like many other organizations, these institutions employ Information and Communication Technology and other internet-based services. However, Academic Institutions in developing countries still lag in incorporating advanced technologies. Al-Shqeerat et al. (2017). This is attributed to inadequate ICT infrastructure, financial constraints, lack of space to meet the high demand in the education sector, the increase of data due to the growing population in Higher Institutions, cost of hardware/software, data alteration/theft, loss of data during migration, limited teaching materials and resources such as books, journals, and libraries, high administrative costs and difficulties in managing large population of learners against small number of lecturers and other violation to server-based ERP systems).

Academic Enterprise Resource Planning (ERP) systems are meant to integrate the various activities, processes, and functions within a Higher Institution in order to streamline the process and to provide real-time, on-demand information needs (Muli & Kimutai, 2015). However, as these activities, processes, and functions continue to grow, more resources are needed to manage the system. The volume of data produced grows every day due to increase in staff members, students, the department as well as academic programmes. Cloud Computing is the delivery of services, servers, storage, databases, networking, software, and more, over the Internet, to offer faster innovation and flexible resources (Kattimani & Mallinath, 2017).

In order to adapt to these emerging trends, and Academic ERP system must be migrated to the cloud-computing platform, and such platforms offer improved security and privacy, reduce hardware, software procurement, and maintenance costs. It also serves as a reliable backup for future reference in the event of disasters. Never the less despite the numerous advantages presented by cloud computing, Higher Institutions continue to worry about the security and privacy of their data/information in the cloud (Venkatachalam & Arts, 2017). Hence, this thesis proposes a security and privacy model which will help to secure data/information while implementing or migrating from server-based to cloud-based ERP system.

1.1 Background of the study

The Internet is evolving rapidly, from a traditional medium of merely providing information to users, to an indispensable requirement for the users who want to store data, perform computing and even run software applications at any time from any part of the world. This is possible with the advent of technologies such as "Cloud Computing" which is considered to be the fifth generation of computing after client-server computing, mainframe computing, personal computing and the web (Alzaid & Albazzaz, 2013; Rajan & Jairath, 2011; Khmelevsky & Voytenko, 2010). Cloud computing can be viewed as a technology that enables users to gain computing facilities such as data storage and software services via the Internet (AlCattan, 2014; Benton & Negm, 2010). Hence, cloud computing technology allows students to learn, collaborate, and share information online (Rao & Challa, 2013; Razak, 2009).

Cloud computing promises to deliver all IT services on-demand whereby enabling clients to only pay for the specific amounting of resources they use, or in other words, follow the pay-as-you-go pricing model (Sachdeva et al., 2011; Benton & Negm, 2010). Cloud computing is considered as a promising technology to higher institutions that will improve the performance and overcome the excessive cost related to the IT resources. Many organizations around the world, including higher institutions, have realized the advantages of cloud-computing and consequently aspire to move all their services to the cloud due to its numerous characteristics such as availability, scalability, agility, elasticity, and reliability for on-demand services in order to make teaching, learning, and research more accessible.

The fast-growing interest and application of cloud computing, specifically in education, present an opportunity for both students and lecturers to enhance their productivity (Badie, Hussin, & Dahlan, 2014; Tejal & Mathur, 2014; Gital & Zambuk, 2011). This is supported by various studies that present benefits associated with cloud services (Gupta & Thakur, 2014; Truong, Pham, Thoai, & Dustdar, 2012). The benefits include low barriers to entry, low costs, increased mobility, scalability, improving security, active compliance, collaboration among users of cloud-based services, anywhere/anytime access to software, and cloud-enabled processing power and storage on demand (Park & Ryoo, 2013; Verma & Kaushal, 2011).

Implementation of the cloud computing services in the education settings remain at the initial stage of development; existing research recognizes several advantages that can be gained by using cloud

computing services in educational institutions. González-Martínez et al. (2015) further documented the benefits of cloud computing for educational institutions concerning the flexible of learning environments; the availability of online applications to support education; computing-intensive support for learning, teaching, as well as evaluation; support for mobile learning; the scalability of learning systems and applications; and cost savings. Similarly, Tan and Kim (2011) demonstrated how cloud-computing services such as Google Docs were used by a group of students pursuing a Master of Business Administration (MBA) at a University in North-Eastern USA to carry out their projects. They reported that they were helpful to the students, who expressed they would be willing to adopt and use these technologies in the future.

Despite all the advantages presented by cloud computing, it is only recently that educational institutions started adopting the technology. Also, the adoption is usually partial and considered low when compared with other organizations (Okai et al., 2014). According to a survey of post-secondary institutions in the USA, the institutions that implemented cloud-computing do not go beyond 28%, an additional 29% of the institutions only arranged for adopting the technology (CDW, 2011). Also, cloud computing usage in educational institutions accounted for only 4% of the total usage whiles other organizations accounted for the remaining 96% (Mokhtar et al., 2013).

Therefore, migrating from on-premises to cloud-based computing services will represent an opportunity for higher institutions to transform their learning and teaching activities by using cloud computing services that provide a more competitive and robust environment (Tashkandi & Al-Jabri, 2015; AlCattan, 2014). In addition, the current studies in a higher education context did not focus on security and privacy in developing country rather consider factors like academic staff, IT personnel and other decision-makers within the institution (Sabi et al. 2016; Hashim, Hassan, & Hashim, 2015; Irshad & Johar, 2015; Tashkandi & Al-Jabri, 2015).

1.2 Problem statement

It is a known reality that Higher Institutions of learning play a vital role in the growth of societies (Alharthi et al., 2015). Like many other organizations, these institutions employ ICT and other internet-based services. However, Academic Institutions in developing countries still lag in incorporating advanced technologies. This is attributed to inadequate ICT infrastructure, financial constraints (Gamundani et al., 2015; Alghali & Roesnita, 2014)., lack of space to meet the high demand in the education sector. However, the increase of data due to the growing population in

Higher Institutions, cost of hardware/software, data security and privacy, loss of data during migration, limited teaching materials and resources such as books, journals, and libraries, high administrative costs and difficulties in managing large population of learners against small number of lecturers (Gital & Zambuk, 2011; Kanjo, 2008).

Academic Enterprise Resource Planning (ERP) systems are meant to integrate the separate activities, processes, and functions within a higher institution to help streamline the process and to provide real-time, on-demand information needs (Murphy, 2016). The volume of data produced by academic institutions grows every day (Surjeet et al., 2012). Due to the increasing numbers of staff, students, departments, and programs, this continuous growth requires continuous scaling and improvement of the academic ERP system. Therefore, to adapt to this continuous growth, the system should be constructed based on a cloud computing platform, as this will improve the security of the system, software procurement (Shawish & Salama, 2014; Sen, 2013; Chandra & Borah, 2012), serve as a reliable backup for future use should in an invent of natural disaster, prevent against changing of student marks without authorization and other violation to on-premise ERP system. Cloud computing technology helps in solving several futuristic securities, increasing the volume of data requirements of server-based ERP implementation (Goel et al., 2011).

The security and privacy model that has been proposed will be such in which once data are entered into the cloud system and saved, it can never be modified by any user. The security procedure for any modification to take place will be carried out by only ONE chief system administrator, in which the modified copy will be saved as a modified copy leaving the original copy for an audit trail.

1.3 General objective

The general objective of this study is to develop a security and privacy model for cloud-based Enterprise Resource Planning for Kampala International University.

1.4 Specific objectives

1. To study the current server-based ERP system used in a higher institution.
2. To develop a security and privacy model for cloud-based ERP.
3. To validate the developed model.

1.5 Research questions

The primary research question is how to come up with a security and privacy model for cloud-based enterprise resource planning for Kampala International University?

The questions are as follows:

1. What is the current server-based ERP system used in a higher institution?
2. How can the security and privacy model for cloud-based ERP be developed?
3. How to validate the developed model?

1.6 Significance of the study

The future of Information Technology in education is anticipated to zero around accessing resources for learning, teaching, and collaboration (González-Martínez et al. 2015). This point to cloud computing as the future of technology in education. The developed model, when implemented and integrated, will help learners to use cloud services to aid independent learning and study in their way from anywhere.

With cloud computing, lecturers and students can be connected with each other within and outside their campuses, and classrooms can be everywhere since educational resources will be available around the clock as you only pay for what you use, collaboration can be achieved using shared applications such as Google Apps and Office 365 which allow students and teachers to work on the same documents from anywhere in the world.

Cloud computing architectures have a positive impact on e-learning solutions, which is the emerging aspect of distance education offered by many higher institutions. Such systems require infrastructure improvements, resources for maintenance, incompatibilities between systems hardware, and software resources. The best solution is migrating to cloud for cheap, quickly scale up or scale down as demands, also provide advanced strategies to ensure that database mining is generated, critical data is backed up, protected in a secure and safe location.

The study proposes a security infrastructure whereby once an authenticated user enters data into the system, the data cannot be modified by any other user apart from the ONE chief system administrator. Any other modification, if necessary, will be considered as a modified copy and will

be identified, presented, and printed as such. The first saved copy is considered the original copy and is tendered for auditing purposes.

This model will be very significant in maintaining internal consistency. Also, the identified factors, when taking into consideration during development, migration, and implementation of cloud computing services by the cloud applications provider/users, will significantly influence the adoption rate of the technology by decision-makers.

Furthermore, the results of this research will benefit decision-makers, staff, students, and researchers who have an interest in data and information security. The problem of data theft, alteration of results, deliberate deletion of data, which are some of the security challenges in most higher institutions, can be prevented by using pay as you use.

1.7 Scope of the study

1.7.1 Geographical scope

This study was conducted at Kampala International University (Main campus), Uganda, mainly because the main campus has the most significant number of staff (academic and non-academic staff) and has server-based ERP.

1.7.2 Context scope

The focal point of this research is to develop a security and privacy model for cloud-based Enterprise Resource Planning for Kampala International University. The technological infrastructure required for the successful implementation, migration, security, privacy, and intertwined challenges was analyzed using the interview as a data collection method.

The validity of the developed model was evaluated in order to demonstrate the effectiveness of the proposed model.

1.7.3 Time scope

The study started from the elicitation stage from December 2017 to June 2019.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

The purpose of this research is to come up with a security and privacy model that can be used in the implementation of a cloud-based ERP system in higher institutions. Chapter one introduced the research studied by stating the objectives of the study, the research question, and its importance. It is in this chapter where available articles, books, journals, and the web is being reviewed in the domain of cloud computing, cloud-based ERP, cloud security, and implementation. This chapter look at some models for implementing server-based and cloud-based ERP systems, which have previously developed.

2.1 History of cloud computing

Fundamentally, the notion of cloud computing has been in existence since the 1950s, during the mainframe computing age (Bhatiasevi & Naglis, 2016). In mainframe computing, multiple users access a central computer using terminals (Neto, 2014). At that time, the cost of purchasing and maintaining mainframe computers was very high, making it impractical for each user to own one. The storage and processing capacity of the mainframes were also too large for a typical user. As a result, the idea of shared access to mainframe computers evolved (Almishal & Youssef, 2014; Neto, 2014). In the 1960s, a computer scientist John McCarthy who is recognized as the founder of the time-sharing concept proposed that computing power and application might in the future be delivered as a public utility like electricity and water. This idea plays a significant role in the formation of today's cloud computing (Mohamed, 2009; Foster, Zhao, Raicu, & Lu, 2008). Another idea that contributed to the development of cloud computing is the "Intergalactic Computer Network" proposed by Joseph Carl Robnett Licklider in the early 1960s (Hauben & Hauben, 1998). Intergalactic Computer Network is a networking concept whereby people will be globally interconnected in order to access programs and data from anywhere. This idea later transformed into ARPANET in the late 1960s, and finally, in the 1970s it changed into today's Internet (Mohamed, 2009; Hauben & Hauben, 1998; Judy, 1995). Similarly, in the 1970s, the concept of virtual machines was developed in which virtualization software was used to run several operating systems on a computer. The virtualization advancement of time-sharing in the

mainframe era because it allows "multiple distinct computing environments to reside on one physical environment" (Neto,2014). It was in the late 1970s that people started using the term "client-server" (Writer, 2015). Client-server represents a model where clients access applications and data from a computer called a server over a network. In the client-server model, the client initiates the connection while the server replies by providing the requested data access to the requested application (Dye, McDonald, & Rufi, 2008). Personal computers were also introduced during this era (Mowery & Simcoe, 2002).

Furthermore, telecommunication companies were generally known to provide data connection services single dedicated point-to-point data connections, but in the 1990s, they began to offer the service as a Virtual Private Network (VPN) with similar quality of service cheaply (Neto, 2014). The design of the VPN was to enable multiple users to share the same physical infrastructure (Neto, 2014). The year 1999 marked the beginning of cloud services provisioning companies such as Salesforce.com, Google, and Netflix. Salesforce.com was the first company that provided enterprise applications from its website (Writer, 2015). Google launched a fledgling search service, while Netflix started its service of mailing Digital Video Disks (Writer,2015). Later, Amazon developed Amazon Web Services (AWS) in 2002 and officially launched its commercial web service called Elastic Compute (EC2) in 2006 (Writer, 2015; Pallis, 2010). AWS provides customers with the ability to store their data and information, and also human intelligence services that enable users to perform tasks using Amazon Mechanical Turk (Writer, 2015; Mohamed, 2009). EC2 allows individual customers and companies to run their computer applications on rented computers (Mohamed, 2009). Subsequently, Amazon launched Amazon Simple Storage Service (S3) (Mohamed, 2009). S3 is one of the popular and pioneer online storage services that can be accessed through web services interfaces such as Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) (Buyya et al. 2009). According to Mohamed (2009), EC2/S3 is the first broadly accessible cloud infrastructure service. S3 is believed to provide high computing capacity faster and cheaper than a local server deployed in a company (Sommer, 2014).

The evolution of cloud computing can be viewed from the history of computing perspective, which is divided into six stages (Prasad, Naik, & Bapuji, 2013; Girdhar, 2010; Voas & Zhang, 2009).

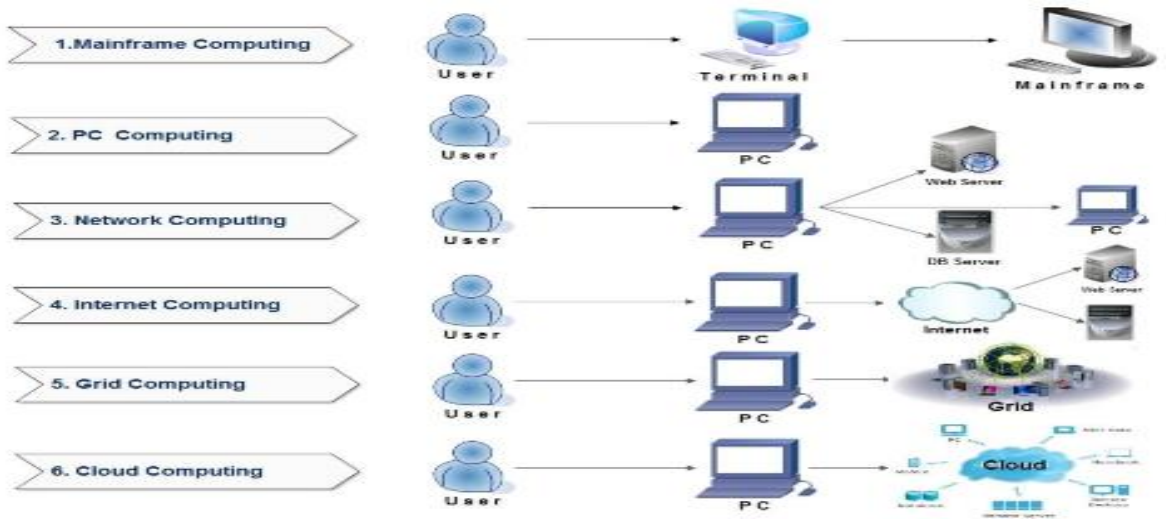

Figure 1: Six stages of computing paradigms (Source: Prasad et al., 2013)

During phase 1, multiple users were allowed to access a powerful mainframe using "dummy" terminals that were slightly more than keyboards and monitors (Voas &Zhang, 2009). During phase 2, Personal Computers (PCs) became powerful enough to satisfy the majority of a user's needs (Verma, Dutta, Chaulya, Singh, & Prasad, 2013; Furht, 2010). In phase 3, computers (PCs, servers, and laptops) were locally networked for improved performance by sharing resources (Verma et al., 2013; Girdhar, 2010; Voas & Zhang, 2009). Resources sharing was further improved in phase 4 by connecting multiple local networks to form a global network (Internet). This enabled the running of various applications and accessing resources remotely (Furht, 2010). The concept of grid computing was introduced during phase 5, which utilized the idea of distributed computing to share computing power and storage (Singh & Hemalatha, 2012; Girdhar, 2010). Grid computing led to the emergence of cloud computing in phase 6, where computing resources are provided on demand to the users as a service over the Internet (Verma et al., 2013; A. Singh & Hemalatha, 2012; Voas & Zhang, 2009).

2.1.1 Definition of cloud-computing

Cloud computing is gaining more attention from individuals and researchers. This perhaps is one of the reasons why it is defined in many ways (Wang et al., 2008). Vaquero, Rodero-Merino, Caceres, and Lindner (2009, p. 51) these researchers reviewed so many definitions from twenty cloud definitions from different researchers and came up with a summarized definition as "a large

pool of accessible and usable visualized resources (such as hardware, development platforms, and services). These resources are dynamically reconfigured to regulate to a variable load (scale), also allowing for optimum resource utilization. This pool of resources is usually exploited by a pay-per-use model within which guarantees square measure offered by the Infrastructure supplier by suggests that of tailored Service-Level Agreements (SLAs). Cloud computing is additionally outlined as a sort of parallel and distributed system consisting of a group of interconnected and visualized computers that square measure dynamically provisioned and given joined or additional unified computing resources based on service-level agreements established through negotiation between the service supplier and consumers" (Buyya et al., 2009, p. 601). Furthermore, the National Institute of Standards and Technology (NIST) described cloud-computing in a comprehensive, formal and standard way as "a model for convenient, sanctioning gift and on-demand network access to a pool of configurable computing resources (e.g., storage, services, server, networks and applications) that can be chop-chop provisioned and discharged with the smallest management effort or service supplier interaction" (Mell & Grance, 2011, p. 2). Thus, cloud computing can be defined as a model that provides computing resources as a service. The resources include applications, storage, networks, and other services (Mell & Grance, 2011; Trovati et al., 2015). As shown in Figure 2, the cloud-computing model described by Mell and Grance (2011) comprises five fundamental characteristics, three service models, as well as four deployment models.

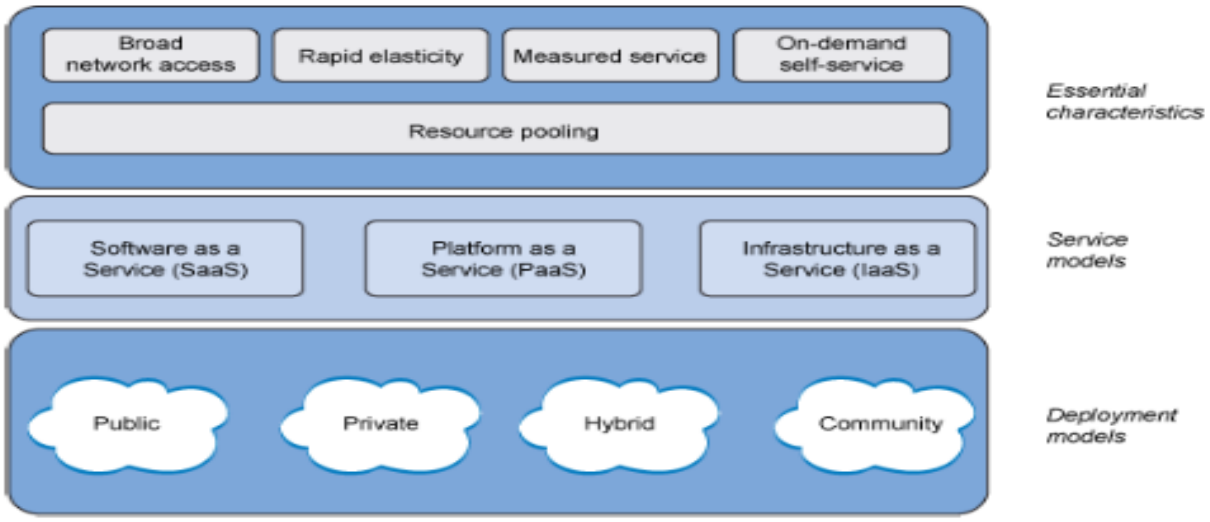

Figure 2: Pictorial representation of the cloud-computing model (Source: Markey, 2013)

Moreover, there is a misconception about the distinction between cloud computing and terms like cluster computing and grid computing. Cluster computing determined "a variety of parallel and distributed system that consists of a set of complete, interconnected computers operating along as one integrated computing resource" (Buyya et al., 2009, p. 601). It is pertinent to note that cluster computing is generally centralized setup with a focus on utilizing parallel processing power and load balancing in order to improve fault tolerance, performance, and availability of service (Kaur & Rai, 2014; Buyya et al., 2009; Baker, 2011). Similarly, grid computing technology is a model that shares the resources of multiple computers in order to perform a task (Hashemi & Bardsiri, 2012). Buyya et al. (2009, p. 601) made public grid computing as "a form of parallel and distributed system that allows the sharing, selection, and aggregation of geographically distributed 'autonomous' resources dynamically at run time betting on their handiness, capability, performance, cost, and users' quality-of-service necessities."

2.1.2 Components of cloud computing

Cloud computing technology consists of various components that play significant roles in delivering functional cloud-computing services. These components are clients, data centers, and distributed servers, as shown in the Figure below.

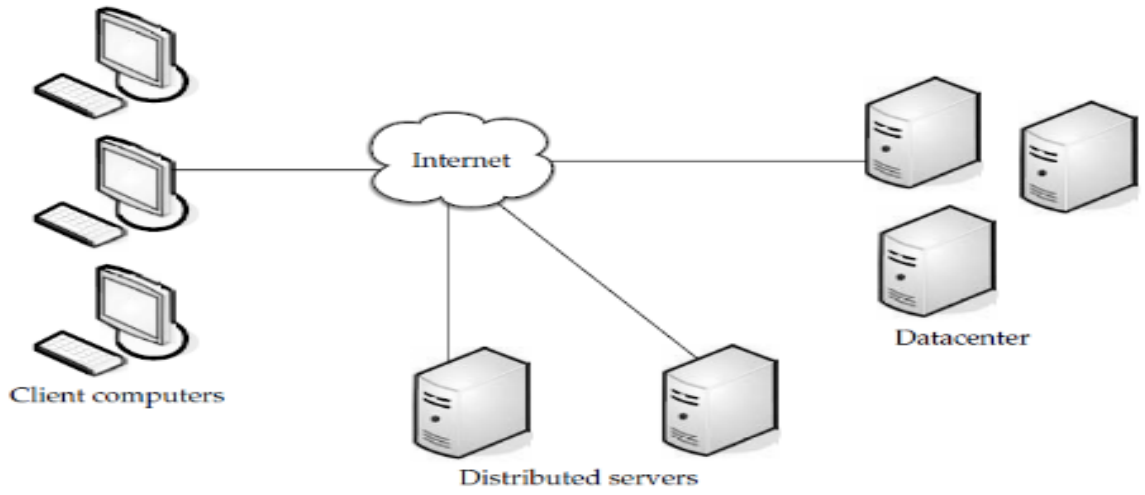

Figure 3: Components of cloud computing (Source: Velte et al., 2010)

From figure 3 above, Clients are computers and mobile devices that are used by end-users to access cloud computing services. Clients are further categorized into three, namely mobile, thin, and thick clients (Hung et al., 2014; Velte et al., 2010). Mobile clients are mobile devices such as Personal

Digital Assistants (PDAs)and smartphones. Thin clients represent computers that are used to display information only as they do not have hard drives and, as such, are not processing any information. Thin clients are being used nowadays because of their benefits, which include low hardware and IT cost, increased security, and less noise and power consumption. Thick clients are ordinary computers like PC that use interfaces such as a browser to connect to cloud services (Velte et al., 2010). The data center is generally a facility or a room with a group of servers that host the cloud service applications. The servers are either physical or virtual, depending on the setup. Multiple virtual servers can be created on a single physical server using virtualization software (Tsai, Sun, & Balasooriya, 2010; Velte et al., 2010; Zhang, Cheng, & Boutaba, 2010). Distributed servers are multiple servers dispersed over a wide geographic location (Velte et al., 2010). Although the servers are not in the same location, they appear to the consumers as if they are together. The function of these servers is to increase the reliability, efficiency, flexibility, and scalability of the cloud services (Velte et al., 2010).

2.1.3 Characteristics of cloud computing

Understanding the fundamental characteristics of cloud-computing technology is imperative because of its growing need for various organizations. Practically, there are five fundamental characteristics of cloud computing, as suggested and defined by NIST, which are: on-demand self-service, rapid elasticity, resource pooling, broad network access, as well as measured service (Mell & Grance, 2011).

2.1.3.1 On-demand self-service

Computing resources such as applications and storage can be easily requested and acquired by a consumer alone without human interaction with the service provider. A consumer usually requests for service when needed, and as such, the billing is on the pay-for-what-you-use basis (Mell & Grance, 2011; Verma & Kaushal, 2011).

2.1.3.2 Broad network access

Resources can be accessed at any time from anywhere through the Internet. A consumer can use any network-enabled device like a tablet, mobile phone, laptop, or PC to access the service (Pramod, Muppalla, & Srinivasa, 2013; Sajid & Raza, 2013; Mell & Grance, 2011). This capability enables consumers to use the resources and services anywhere they go and at any time.

2.1.3.3 Resource pooling

The resources provided by cloud service providers are pooled so that it can be used by multiple consumers at the same time from anywhere using a multi-tenant model (Verma & Kaushal, 2011). Generally, consumers do not know the exact physical location of the resources, and they have no control over the location, although they may know the address of the provider (Sajid & Raza, 2013; Mell & Grance, 2011).

2.1.3.4 Rapid elasticity

The cloud services are flexible and scalable. That is to say, the capacity of the delivered resources can be easily and quickly (mostly automatically) scaled up or down. Also, a consumer can add or remove resources in order to meet his/her needs (Pramod et al., 2013; Sajid & Raza, 2013; Mell & Grance, 2011; Verma & Kaushal, 2011).

2.1.3.5 Measured service

The resources are monitored, controlled, and reported for proper optimization using metering, load balancing, and automated resource allocation (Mell & Grance, 2011; A. Verma & Kaushal, 2011). This capability ensures transparency and allows consumers to pay for only the resources required. In this situation, the resources will not be wasted as in the case when the resources are provided and managed by an in-house server.

2.2 Service models of cloud computing

Cloud computing has different service models that describe the type of services and capabilities that can be delivered by cloud service providers. The three popular models of cloud service are Software as a Service (SaaS), Platform as a Service (PaaS), as well as Infrastructure as a Service (IaaS) (Sajid & Raza, 2013; S. Hashemi, 2013; Mell & Grance, 2011; Verma & Kaushal,2011; Dillon, Wu, & Chang, 2010). The figure below shows cloud computing delivery models, and the table compares the models of SaaS, PaaS, and IaaS.

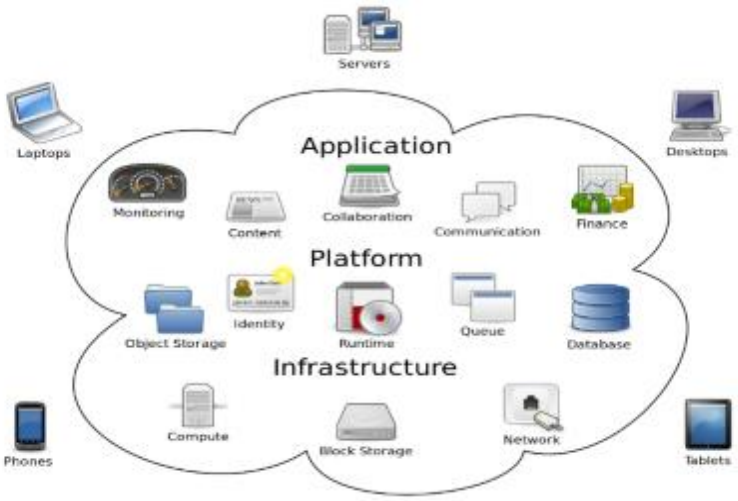

Figure 4: Cloud computing delivery models (Source: Sajid & Raza, 2013)

The table below compares the models of SaaS, PaaS, and IaaS.

Table 1: Cloud service models (Source: Tian and Zhao, 2015)

Classification	**Service Type**	**Flexibility/ Generality**	**Difficulty Level**	**Scale and Example**
IaaS	Basic computing, storage, network resources	High	Difficult	Large, Amazon EC2
PaaS	Application hosting environment	Middle	Easy	Middle, Google App Engine
SaaS	Application with a specific function	Low	Middle	Small, Salesforce CRM.

2.2.1 Infrastructure as a service (IaaS)

Infrastructure as a service is computing resources model or hardware such as networks, servers for processing and storage are provided to the consumers to deploy and run software such as applications and operating systems (Verma & Kaushal, 2011; Wiedemann & Strebel, 2011). This type of service is similar to have a server in the form of the virtual machine in a cloud (Milić, Simić, & Milutinović,2014; Pramod et al., 2013). The consumers have no control over the cloud infrastructure, but they can manage the deployed applications, and other delivered resources (Mell & Grance, 2011). The function of IaaS is similar to the data center where the providers manage

and control the data centers, and consumers deploy and manage their applications (Verma et al., 2013). This capability allows individuals as well as organizations to hire these resources instead of spending money to buy and manage servers that deliver the resources (Sukumaran, 2011). IaaS is usually compared with hosting, but in IaaS, users do not enter into a long-term deal with the providers, and the resources are provisioned on-demand (Bhardwaj, Jain, & Jain, 2010). Famous examples of IaaS are Amazon's S3 storage service, Rackspace Cloud Servers, OpenNebula, Joyent, and Terremark (Marston et al., 2011; Verma & Kaushal, 2011; Dillon et al., 2010). The figure below shows the separate responsibilities of the service provider and client in the cloud service environment.

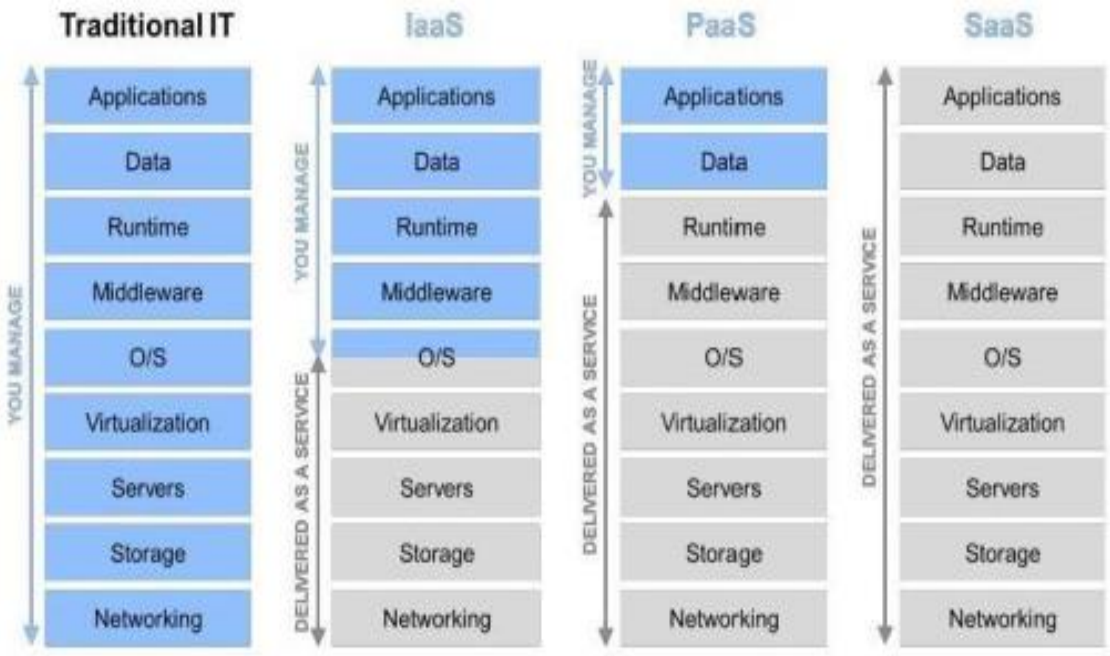

Figure 5: Cloud service model and Separation of Responsibilities (Source: Tian and Zhao, 2015)

IaaS Characteristics: The characteristics of IaaS include (Gilani et al., 2015; L. Wei et al., 2014)

1. It allows for many users on a single hardware.
2. Resources available as a service.
3. It scales capabilities are Dynamic.
4. The cost varies depending on the available infrastructure selection.

IaaS Suitability: IaaS suitable for the following: (Gilani et al., 2015; L. Wei et al., 2014)

1. Organizations that need complete control over their software, e.g., for high performing applications.
2. Startups and small companies that do not wish to spend money and time on procuring hardware and software.
3. Growing organizations not yet sure which applications they will need, or that expect to evolve unpredictably, and hence do not want to commit to a specific infrastructure.
4. Services that experience volatile demands

IaaS Examples: samples of IaaS embrace Amazon net Services (AWS), Cisco Metapod, Microsoft Azure, Google work out Engine (GCE).

2.2.2 Platform as a service (PaaS)

Platform as a service is a model whereby Application Program Interfaces (APIs) or development environments are provided where consumers can build and deploy their applications on the cloud (Pramod et al., 2013; Tan & Kim, 2011; Verma & Kaushal, 2011). The consumers can manage their implemented applications and can change some hosting settings, but they have no control over the cloud infrastructure (Mell & Grance, 2011). Examples of PaaS include Google App Engine, Microsoft's Azure Services Platform, Amazon's Relational Database Services, Amazon Web Services (AWS), Salesforce's Force.com, Rackspace Cloud Sites, and International Business Machines (IBM) Cloudburst (Gupta, Seetharaman, & Raj, 2013; Dillon et al., 2010). Different providers may use different programming languages to build an environment where consumers can deploy their applications (Androcec, 2013). For instance, Google AppEngine used Java and Python, and Windows Azure used DotNet (Vecchiola, Chu, & Buyya, 2009). This a perhaps one of the challenges that consumers may face when switching from one provider to another (Androcec, 2013; Islam, Morshed, & Goswami, 2013).

PaaS Characteristics: The characteristics of PaaS include: (Hoyer and Obel, 2018)

1. A virtualization technology builds on top of PaaS enables acquiring resources on-demand, and scaling them up/down as needed.
2. Different application execution services and application development to facilitate discovery phase, design phase, development phase, QA/testing phase, deployment phase, and hosting of software applications in an integrated development environment.

3. It allows for multiple users to share the same development environment.
4. It allows for integrated web services and databases.
5. The billing and subscription managed by cloud-computing tools.

PaaS Suitability: PaaS is suitable for the following: (Hoyer and Obel, 2018)

1. Multiple developers can work on the same developed product.
2. Organizations following the Agile Methodology for software development; PaaS cease the difficulties associated with the rapid development and iteration of an application.
3. Organizations that wish to expand their capital investment; PaaS reduces the spending on computing infrastructure as well as application development and execution. Enterprise PaaS Examples: Apprenda.

2.2.3 Software as a service (SaaS)

This is the most commonly known cloud service model that allows consumers to use providers' software applications over the Internet (Pramod et al., 2013; Verma et al., 2013). SaaS applications can be accessed anytime from anywhere using the thin client interfaces like a web browser or programming interface (Mutiara, Refianti, & Witono, 2014). SaaS enables consumers to use the software when they require them without the need to buy and maintain such software or procure and maintain a server (Ambrose & Chiravuri,2010). Consumers, in this case, have no control over the cloud infrastructure and the application, but they may be allowed to configure and change basic user-specific settings (Mell & Grance, 2011). SaaS is similar to renting software for a limited time rather than buying it because the software will be provided on demand, and the consumers will only pay for what they use (Ojala, 2013). Examples of this service are Google Docs, Salesforce CRM, and Trend Micro (Chang, Wills, & Roure,2010).

Furthermore, there are other service models that are considered as unique kinds of models (Sabahi, 2011a). They are: Data storage as a service (DaaS) for delivery of storage, Hardware as a Service (HaaS) for delivery of hardware, Identity and Policy Management as a Service (IPMaaS) for managing the identity and control policy of the consumer, Network as a Service (NaaS) for delivery of virtualized network, Business Process as a Service (BPaaS) for delivery of business process outsourcing, Database as a Service (DBaaS) for database outsourcing, Sensing as a Service (S2aaS) for delivery of sensing applications, Middleware as a Service (MWaaS) for outsourcing

middleware solutions like application server, databases, and messaging. It can be noticed that, HaaS, DaaS, and NaaS are particular type of IaaS (Sheng et al. 2013; Verma et al., 2013; IBM Global Technology Services, 2012; Moscato, Aversa, Di Martino, Fortis, & Munteanu, 2011; Dillon et al., 2010; Lehner & Sattler, 2010). The cloud service models are provided by cloud service providers, which are vendors who lease cloud services to customers on-demand (Almishal & Youssef, 2014).

SaaS Characteristics: The characteristics of SaaS include: (Gilani, Salam, and Ul H aq, 2015; Wei et al., 2014).

1. Software hosted on a distant server, and always accessible through a web browser over the Internet.
2. Application managed from a central location.
3. Application users do not have to worry about software or hardware.
4. Any integration with third-party applications is done through APIs.

SaaS Suitability: SaaS is suitable for the following: (Gilani et al., 2015; L. Wei et al., 2014).

1. Applications where the demands spike or fall significantly. For example, tax software is high demand during the tax in the filing season, and hotel reservations see a spike during holiday seasons, and so on.
2. Applications that need net moreover as mobile access. Examples include sales management software, customer relationship management systems.
3. Short-term projects that require collaboration. The pay-as-you-go model makes it is convenient to quickly discover a supportive setting and quickly close it down.
4. An organization that wants to quickly start e-commerce sites without worrying about software updates and server configurations.

SaaS Examples: Cisco WebEx, Salesforce, Citrix GoToMeeting, Google Apps, Workday, Concur.

2.3 Information on security and privacy in clouds

Security can be defined as follows (Ramey and Rao, 2011): “Security is the right not to have one’s activities adversely affected via meddling with one’s objects.” In an equally succinct way, we can define privacy as follows (Ramey and Rao, 2011): “Privacy is the right to have information about

oneself left alone." Similarly, Rocha et al. in 2011 define privacy as the selective control of access to "self." Selective control refers to the process where individuals control their interaction and information exchange with others. Individually tries to control their privacy by controlling their openness to others. Pearson, in 2009, explains that the level of the openness between individuals is determined by their relationship and the value given to the information safeguarded. Privacy will usually be delineated because of the dynamic method whereby people regulate the degree of their openness to others.

Classic "CIA" Security Triad. A classic definition of security in terms of its essential characteristics specifies it in terms of the CIA triad; the acronym "CIA" stands for confidentiality, integrity, and availability which are the three critical requirements for any secure system (Padron, 2017; Zhang et al.., 2010).

They are defined as follows:

2.3.1 Confidentiality

It is the power to cover information from those folks unauthorized to look at it. It is the premise of many security mechanisms protective not solely information, however different resources (The CIA Principle, 2018).

2.3.2 Integrity

It is the ability to maintain the expected state of data/information either on retrieval, in transit, or the storage state (Padron, 2017).

2.3.3 Availability

It ensures that a resource is quickly accessible to the approved user upon the user's request (Singh et al., 2016).

This model is applicable across the whole subject of security and privacy analysis, from access to a user's Internet history to the security of encrypted data across the Internet. (Singh et al., 2016). Security and privacy in clouds over the years, many researchers have surveyed and studied the issues of privacy and security in cloud environments. To better comprehend those problems and their connections, technology researchers and experts have taken advantage of different criteria to establish a general impression. Gruschka et al., in 2010, recommend modeling of the security

ecosystem in terms of three cloud system participants: service instance, service user, and the cloud provider. Furthermore, they identify attack categories: user to service, service to the user, user to the cloud, cloud to the user, service to the cloud, and cloud to service. While cloud computing is associated with numerous security and privacy problems, it can be made active by implementing efficient solutions.

2.4 Cloud service models and their security risks

Virtualization technology is a core technology behind cloud infrastructures. Virtualization provides flexibility to maneuver virtual machines in any location for resource optimization. Thus, it creates a challenge to enforce an organization's security and compliance policy since customers are uncertain of the actual physical location of the data and computing resources. As mentioned elsewhere in this research study, cloud service models are classified as 'Software-as-a-Service '(SaaS), 'Platform-as-a-service' (PaaS), and 'Infrastructure-as-a-Service' (IaaS). The figure below shows the SPI risk model.

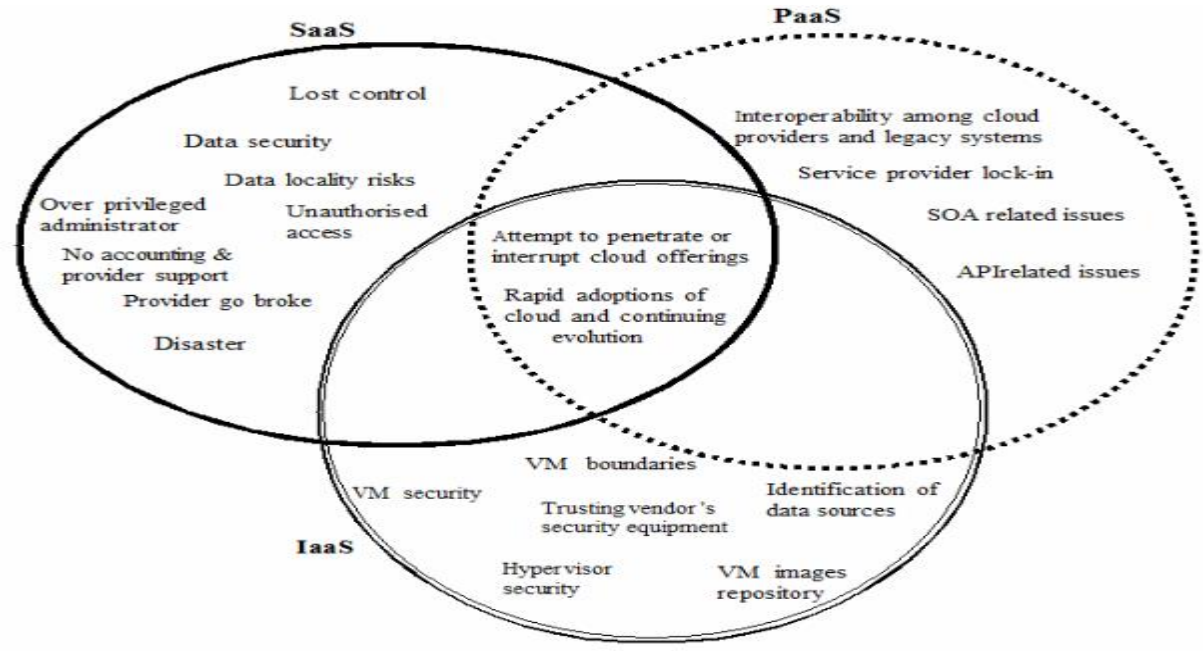

Figure 6: SPI risk models (Source: Brodkin, 2008)

As shown in Figure 6 above, all cloud-computing risk was identified and grouped into the cloud-computing model of SaaS, PaaS, and IaaS. There were two risks identified to be common for all the three models. They are the rapid adoption and evolution of cloud computing and the increasing

risk of cloud computing being targeted by hackers. The main reason being that cloud-computing is dynamic and continuously changing. Changes in the technology, as well as changes in the process, make it is vulnerable to hacking, and policymakers have to keep pace with these changes to come out with the regulation.

2.4.1 Security risks in the SaaS model

This explicit service model provides access to applications that run on a service supplier infrastructure. Services area unit obtainable from numerous many alternative consumer devices via various strategies like an internet browser and mobile app. Examples are web-based email and video conferencing. Here the client does not manage or manage underlying IT infrastructure (Brodkin, 2008).

Possible security issues in SaaS model among others include:

2.4.1.1 Sole dependencies on vendor model

Customers solely depend on cloud service provider security measures and standards. Since cloud supplier in SaaS supports an outsized range of users, it is laborious to create sure that acceptable security measures area unit taken into thought to guard client knowledge and at the same time, also ensure that the customer applications available with proper security when needed. (Brodkin, 2008).

2.4.1.2 Security on the network

Customers are unable to have an accurate picture of the cloud provider systems, and network security behind their slick marketing. Hackers can exploit a weakness in network security, sniffing the packets. Possible threats area unit Man-In-The-Middle (MITM) attack, network penetration, session management weakness, and insecure Secure Socket Layer (SSL) trust settings (Morsy, Grundy & Muller, 2010).

2.4.1.3 Data security

Hackers who specialize in manipulating weakness in the data model to gain unauthorized access to data or application. SaaS is at risk if there are virtual machines operating system flaws, improper access management, cookies, and hidden field manipulation, as well as insecure configurations and storage (Morsy et al., 2010).

2.4.1.4 Identity management

Because of giant customers' base and verities service sort supports by the cloud service provider, it is another challenging task in a cloud environment, and mismanagement of identity control may lead to unauthorized data access. Password management is complicated and turning into less economical as a result of hackers currently have the promptly available tools for cloud and computing capability to bust through word protections (Gefen and Ragowsky, 2005).

2.4.1.5 Data isolation

Encryption may help segregate different users' data alongside with other customers in the shared environment, but it is not an effective cure. Mismanagement (loss of key) of encrypted knowledge will build knowledge entirely unusable, and hinter availability of the encrypted data. Besides this, it is troublesome to controls or outlines body tasks between consumer and cloud suppliers as usually they usually got to work along to accomplish a specific task. Current third-party liabilities protections are vitally attributable to the number of knowledge the cloud suppliers handle build screening quite not possible (Brodkin, 2008).

2.4.1.6 Data locality risks

In a cloud consumer, knowledge might not be physically kept in an exceedingly supply country, maybe knowledge is going to be distributed or keep on the far side the border so international knowledge privacy protections and export restriction law may apply and also increase chances of data leaks due to poor security in different geographic (Subra, 2011).

2.4.1.7 Data integrity

It is troublesome to keep up knowledge integrity over distributed infrastructure like cloud computing. In SaaS, applications area unit multi-tenant hosted by the third party, so it always exposes practicality via protractible language (XML) based mostly Application Programme Interface (APIs). Improper integrity controls at the info level (directly access information bypassing application logic) might lead to many-sided security problems (Morsy et al., 2010).

2.4.1.8 Disaster

Recovery, since system pictures area unit being backed-up and distribute or replicate between multiple sites, it is difficult to make a system recovery when lacking proper procedure and support

from the cloud vendor Disaster recovery process could jeopardize the security of the customer's data (Brodkin, 2008).

2.4.2 Security risks in the PaaS model

In the PaaS model, the service provider provides a platform for the customer (developer) to develop and deploy their own or acquired applications. Often service provider provides an application in programming interface (API) or template-based development engine to build a custom application. The customer does not manage or control the infrastructure such as servers, network, operating system except deployed application and its configuration. This service free-up programmers or IT professionals from the complexness of managing their own IT infrastructure.

Possible specific security risks in PaaS are:

2.4.2.1 Absence of interoperability among cloud providers and legacy systems

Different cloud provider uses a different type of security products and methods to secure their infrastructure and legacy.

2.4.2.2 Service provider lock-in

Various cloud suppliers style their cloud service, mistreatment their proprietary technology, and use security normal or protocol proprietary to their platform. For example, the Microsoft Azure platform is built on dot net, and if a customer needs to move from Microsoft to some open-source platform provided by other vendors, it will be difficult, and conjointly the migration method could cause security problems. Therefore, it is troublesome to maneuver from one supplier to a different one. This scenario could exist in the SaaS model as well (Shinder, 2011).

2.4.2.3 Service-oriented architecture (SOA)

PaaS service model is built on Service Oriented Architecture (SOA) model thus it inherits security issues which exist in SOA models such as DoS attacks, MITM and XML related attacks, dictionary attacks, replay attacks, SQL injection attacks and data entry validation related attacks (Shinder, 2011). SOA threats are also available InGaAs model.

2.4.2.4 Application programming interface (API)

If the Appliance Programming Interface (API) that the client accustomed to manage and move with cloud services is not secured, it could be a result of sending data in the clear text, and that

could cause a security breach. Different API cloud vendors are using a different type of API standard. Applications created with a much different type of APIs could create potential security risks due to incompatibility and integration issues (Morsy et al., 2010).

2.4.3 Security risks IaaS model

This capability provided to the customer is often referred to as "everything-as-a-service. "Generally, it represents the entire virtual infrastructure as a service over the net (includes firewall, RAM, CPU. The purpose of this offering is to replace a customer's server room and network with virtualization technology, and it also contributes to cost reduction and improved flexibility. Major players embody Amazon, Rack space, Savvis, HP, IBM, Sun, and Google. Possible security risks are:

2.4.3.1 Trusting providers underlying security equipment

It is tough for cloud customers to completely perceive the supplier security configuration in core physical level and conjointly making certain that the service supplier configuration normal does not conflict with the customer's own organizations' security policy (CCIA, 2009).

2.4.3.2 Identification of appropriate data sources

It is a challenge to see that information sources square measure relevant for incident detection notably with IaaS (providing intrusion detection for virtual machines while not knowing how to implement inoperative system) and PaaS (providing intrusion detection for net applications while not knowing the sort of applications hosted) (Morsy et al., 2010).

2.4.3.3 Virtual machine (VM) security

Malware, viruses, DOS, memory leaks, and other VM operating systems and various workloads are the most common security threats. The VM's security may be a part of client responsibility in IaaS (Morsy et al., 2010).

2.4.3.4 Security in VM images repository

Unlike a physical server, VMs image is still at risk when it is serviced in the mechanical. It is common practice taking a snapshot of VMs for disaster recovery. Thus, VM images can be under the risk of malicious codes injection when offline, and these VM files could be stolen too. Although the customer is ultimately responsible for the VM security since the vendor is an owner of the physical hardware there is a possibility that clouds provider may copy the existing customers' VM

and reuse for another customer. Another issue in the VM environment is related to VM templates; it is common practice to use a template for rapid deployment of the system, and all these templates may contain the original owner information, which may be re-used for new customers (Morsy et al., 2010).

2.4.3.5 Virtual network security

In IaaS, cloud customers share supplier physical infrastructure with many various customers, which increases the danger level of exploiting vulnerabilities in numerous servers running DHCP, DNS, and IP protocols.

2.4.3.6 Securing VM boundaries

VM servers will be designed with virtual boundaries (isolated from alternative VMs) to supply network property among VM servers for security. Generally, VMs co-exist in a physical server to share CPU, memory, network card, and other resources. Securing VM boundaries fallen under cloud provider responsibility. This misconfiguration and mismanagement could lead to unauthorized access and data leak (NIST, 2009).

2.4.3.7 Hypervisor security

The hypervisor is a 'virtualize system,' which maps a physical server to a virtual server. Therefore, any compromise on hypervisor means that a compromised hosted VMs. The cloud service provider provides the security of the hypervisor, and any vulnerability in hypervisor software inherits security risk in customer VMs (Morsy et al., 2010).

2.5 Deployment models of cloud computing

Cloud computing presents four different types of environments where consumers can choose to deploy their applications (Brohi & Bamiah, 2011; Liu et al., 2011). The four cloud deployment models are a private cloud, public cloud, community cloud, as well as a hybrid cloud (Hashemi, 2013; Sajid & Raza, 2013; Liu et al., 2011; Mell & Grance, 2011; Verma & Kaushal, 2011). Organizations may decide to use one or a combination of these models based on their needs (Skiba, 2011). The figure below shows the deployment model in cloud computing.

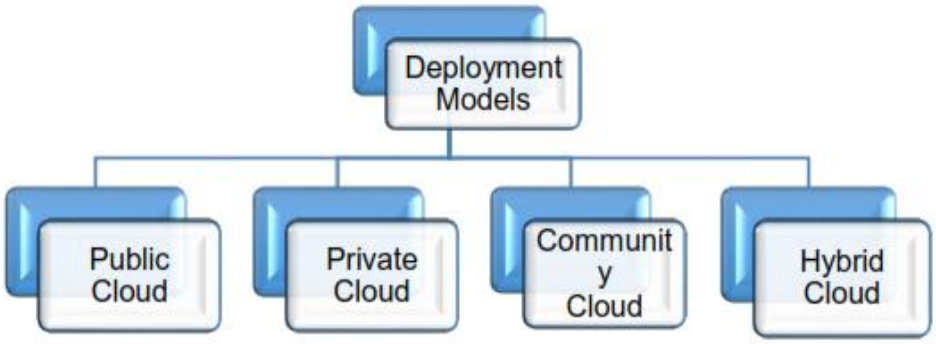

Figure 7: Deployment models for cloud computing (Source: Hashemi, 2013)

2.5.1 Private cloud

In this model, the cloud services are provisioned exclusively for the only organization (Sajid & Raza, 2013). The organization can possess, manage, operate, and host the cloud infrastructure, or it can be managed and hosted by a third party (Dillon et al., 2010). The consumer of the services provided in this model comprises various individuals and departments of the organizations (Mell & Grance, 2011). Organizations generally prefer this model when they want to, for example, utilize their available resources, reduce the cost of data transfer, have total control, and improve the confidentiality and security of their data (Verma & Kaushal, 2011; Dillon et al., 2010). The figure below illustrates the private cloud.

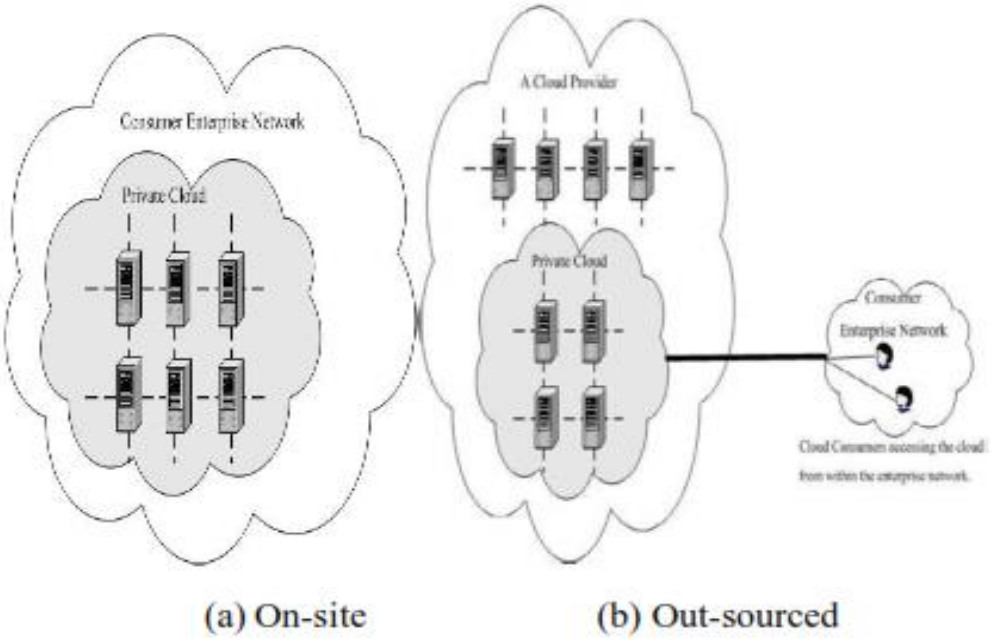

Figure 8: Private clouds (Source: Liu et al., 2011)

The advantages of private clouds include the following ones (Shinder et al. 2013).:

1. Security: The vast array of different deployment types and levels of security within private hosting environments makes this extremely bold statement. The reality on behalf of me is that a non-public cloud is as prone to security risks as a public cloud. The only distinction is that a public cloud is also much enticing to infiltrate than a non-public cloud as there is a wider quantity of knowledge in it.
2. Performance: When an organization deploys a private cloud inside the firewall, this will increase the performance compared to use the public cloud off-premise.
3. Control and Flexibility: Organizations have more control over private clouds and as a result of deploying new applications and make changes, can be done quickly.

There is a unit some disadvantages for personal clouds, including the following ones (Shinder et al. 2013).:

1. Maintenance: Software vendor is responsible for maintaining private cloud by carrying out regular updates that are often associated with modern SaaS applications.
2. Higher Costs: Managing a private cloud is more expensive. Even if the organization purchase the infrastructure or the ISP provides it, it is still costlier to manage than the public cloud.

2.5.2 Community cloud

The cloud services offered in this model is offered to a group of organizations or consumers known as a community (Mell & Grance, 2011). Various organizations that form the community cloud share common concerns like mission, policy, compliance considerations, and security requirements (Sajid & Raza, 2013; Dillon et al., 2010; Mell & Grance, 2011; Verma & Kaushal, 2011). The management and hosting of the cloud infrastructure can be handled by one or more members of the community, a third-party, or both of them (Mell & Grance, 2011). Various community clouds exist, for instance, Healthcare Community Cloud Service™ and the Media Cloud (Carpathia,2015; Henneberger & Luhn, 2010).

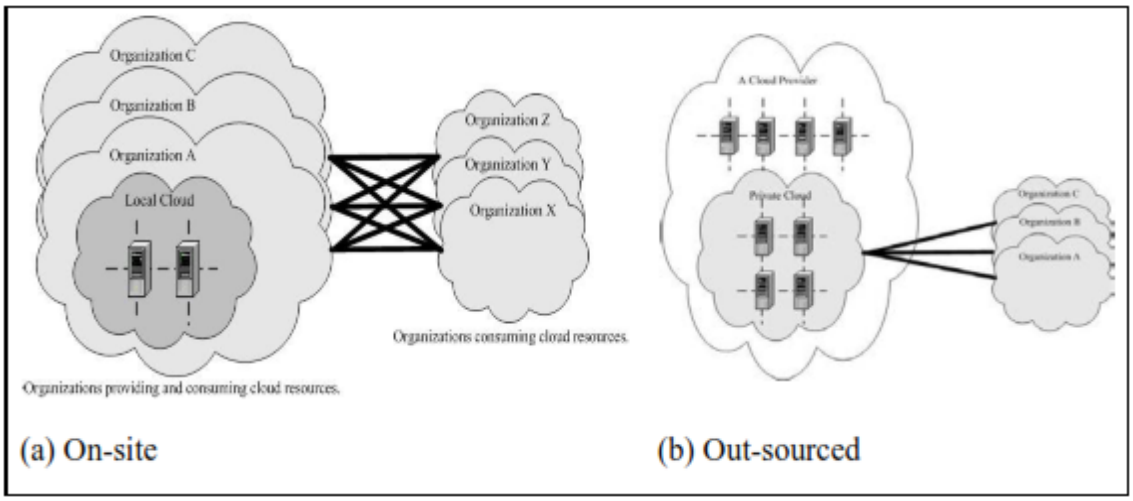

Figure 9: Community cloud (Source: Liu et al., 2011)

2.5.3 Public cloud

This is a deployed model whereby the services are offered to the public (Sajid & Raza, 2013). The cloud infrastructure is managed and hosted by the cloud service providers who are business, academic, or government organizations, or a combination of them (Mell & Grance, 2011). The cloud services may be free to the public or leased and charged based on the pay-as-you-go system (Sabahi,2011b). Consumers share the cloud infrastructure, which makes the cost of the cloud services low since it will be distributed among the consumers (Alsufyani, Safdari, & Chang, 2015; Marston et al., 2011). On the other hand, sharing the infrastructure poses a security and privacy threat (Liu et al., 2011). Amazon EC2, S3, and Google AppEngine are among the popular public cloud services (Ren, Wang, & Wang, 2012; Dillon et al.,2010). The public cloud is shown in the Figure below.

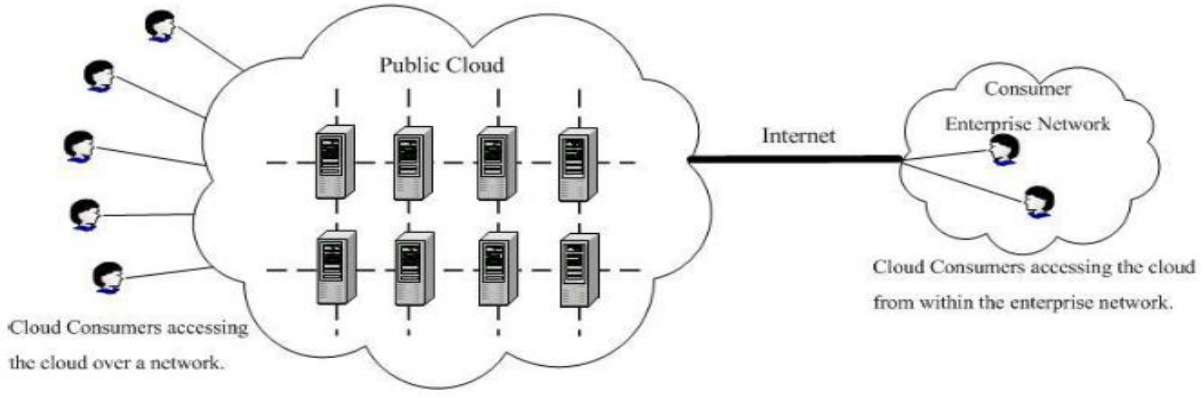

Figure 10: Public cloud (Source: Liu et al., 2011)

The advantages of a public cloud include:

1. Low cost: The benefit of the public cloud is you only pay as you use “pay-as-you-go." So as a corporation grows or shrinks, therefore, do the associated prices. By comparison, a private cloud might require an infrastructure designed to cope with growth (thus more expensive); likewise, costs saved if the needs shrink. Other significant savings area units associated with prices related to the dimensions and work of the in-house IT team.
2. Increased efficiency: Public clouds have specialized staff who carry out maintenance in-case of downtime; infrastructure is less likely to be an issue. On top of this, if applications are hosted by a cloud computing provider, updates are usually managed by the provider, saving upgrading expenses.

Some disadvantages of public cloud are:

1. Wrong provider: There are genuine hazards of picking a wrong public cloud provider. If a supplier does not keep hardware up to date, users could suffer compliance and swiftness problems.
2. Reduced control: As the public cloud is controlled by a cloud-computing the service provider, users do not have as much control as a private cloud.
3. Perceived weaker security: Security might be a downside to a public cloud, but, as proven by the high level of public cloud adoption by some of the world's most prominent organizations, the security concerns are not valid if the public cloud is hosted by a cloud-computing service provider who is aware of security issues, and their impact on customers’ perception (Trovati et al., 2015).

2.5.4 Hybrid cloud

A model is called hybrid when it provides cloud services by combining two or more separate cloud models (private, community, or public) (Sajid & Raza, 2013). The models are bound together using standardized technologies that allow application and data portability, such as “cloud bursting for load-balancing between clouds” (Mell & Grance, 2011, p. 3). Organizations can use the hybrid cloud model when they want to gain the benefits of more than one model simultaneously (Rani & Ranjan, 2014; Zhang et al., 2010). For instance, an organization may host an application with their confidential data on the private cloud and link the application with other software in a public cloud.

In this case, the organization will benefit from the security of the private cloud (Verma & Kaushal, 2011). The hybrid cloud is illustrated in the Figure below.

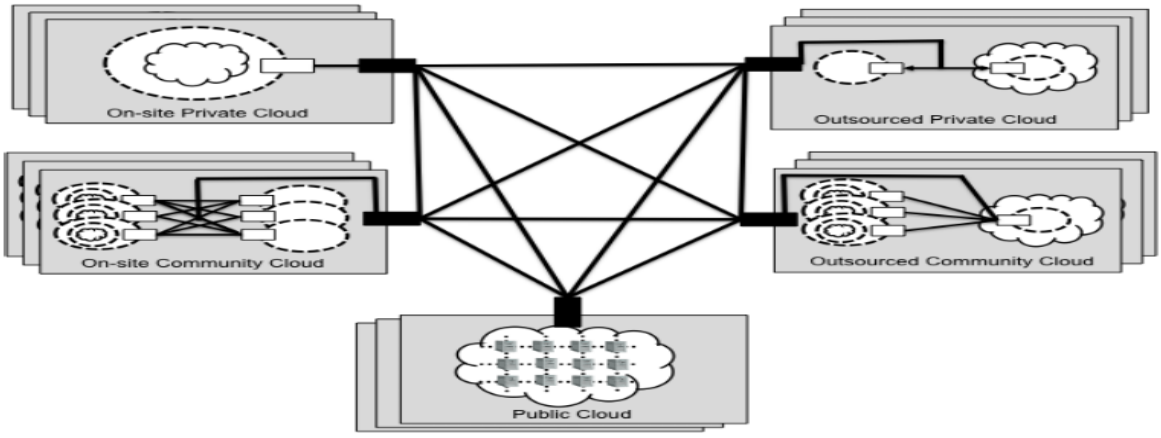

Figure 11: Hybrid cloud (Source: Liu et al., 2011)

The advantages of a public cloud include (Mary Shacklett, 2016):

1. Capacity expansion: When the differential cost of adding capability on-premises is high – assume upgrading power and cooling in a very knowledge center to accommodate extra racks or building a full new knowledge center, a hybrid approach could be a viable different. However, going hybrid does not ought to impact existing operations; choosing a hosted cloud that supports clean metal and lengthening the on-premises network might permit existing technologies, tools, and techniques to be reused.
2. Dev/test: Dev/test workloads are extremely elastic; they are frequently stood up and torn down, and therefore the range of instances at any one time varies wide supported the event part. They are placing these workloads on the hosted cloud permits you to scale capacity to match demand and pay just for what is used.
3. Planned temporary need: Most needs are known in advance, such as new product launches, holidays, peak season, and so forth. When given time to set up and execute, most applications may be scaled.
4. Network optimization: Hosted cloud provides the opportunity to shift the heavy lifting of the network off-premises and, in the process, improves the availability, scalability, and reliability of the connection by leveraging the provider's network investment.

Some disadvantages of public cloud are (Mary Shacklett, 2016):

1. Cost: While the general public cloud offers an attractive choice for its flexibility and comparatively low value to control, building a non-public enterprise cloud needs significant expenditure and might become costly very quickly with all the physical hardware necessary.
2. Security: Cloud computing is not inherently any less secure than traditional computing, and in fact faces fewer attacks, but there are still considerations to take into account when building out a hybrid cloud. The proper precautions must be taken to ensure data is properly protected and that control is maintained by the right people. Additionally, betting on the trade, there is also sure regulative needs that compel knowledge from being held on off-site, which might stop the employment of a public cloud entirely.
3. Data and application integration: Applications and knowledge exist in an exceedingly dependent relationship, with each being useless while not the opposite. Frequently they are chained together. So once considering wherever to store every one of them, it is essential to raise whether or not the infrastructure they're placed on matters. For example, if an application lives in a private cloud and its data lives in an on-premise data center, is the application built in order to access the data remotely? Technologies like copy knowledge virtualization will decouple knowledge from infrastructure and create this downside less of a headache.
4. Compatibility: Compatibility across infrastructure will prove itself to be a significant issue once building a hybrid cloud. With twin levels of infrastructure, a personal cloud the corporate controls, and a public one that it does not, the possibilities area unit that they will be running completely different stacks.
5. Networking: It is necessary to think about the information measure usage might they take abreast of the network and whether or not it could cause issues in bottlenecking alternative applications.

2.6 Local ERP VS Cloud ERP

The table below shows the comparison between server-based ERP and cloud-based ERP for better clarity

Table 2: Local ERP VS Cloud ERP

FACTOR	Local ERP	Cloud ERP
Deployment	Local Server	Cloud Server
Reduced server cost	Low costs	High costs
Implementation	High	Low
Ongoing costs	Relatively high	Low
Control over ERP	Easily controllable	Relatively tough to control.
Integration	Dependent on marketer	Can be managed centrally
Licensing costs	High	Low
ERP module update	Costly	Low-cost
Internet needed	No	Yes
Version	Advanced	Simple

From the table above considering different factor to help analyze the difference between and cloud-based academic ERP, it is clear that cloud-based ERP system has numerous advantage that local ERP except for cost which clouds service provider gives an option of pay as you use and for the case of needing internet before it can be accessed.

2.7 Multilevel security models

The researcher studied previously developed security models as a benchmark to help develop a secure model for the higher institution.

The MLS model was initially designed to support the computer systems in the military sector and to protect the security and their database. The information in MLS is divided into four different security levels based on the information importance and the degree of its sensitive. From low to high grade, the levels contain unclassified level, confidential level, deep level, and top-secret level (Rose and Fogarty, 2006).

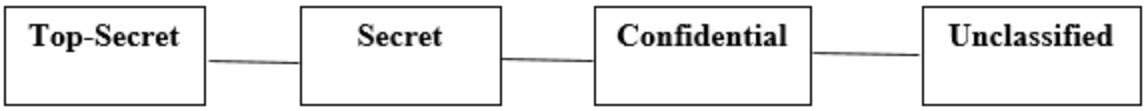

Figure 12: Security levels in multilevel security (Source: Rose and Fogarty, 2006)

MLS systems are essential because:

1. A large amount of research has been done in it because of military funding for computer science in the USA.
2. Originally multilevel concepts were developed to support confidentiality in military applications; however, now multilevel integrity policies are using by many commercial systems.
3. Recently, some products like Red Hat Linux and Microsoft Vista have started to use mandatory access control mechanisms (Rose and Fogarty, 2006).

2.7.1 Analyzing of Multilevel Security Models

A security model is a symbolic representation of a policy. It delineates the requirements of the policymakers into a set of rules that are to be followed by a computer system. It takes the requirement of the policy and supplies the requirement mathematical formulas, relationships, and structure to go after to achieve the policy goal. There are three multilevel security models which are discussed and analyzed as follow:

2.7.1.1 Bell-LaPadula model

Bell-LaPadula Model (BLP) is the most common and frequently multilevel security model, which is used by a computer (Bell and Lapadula 1973). This model was designed in 1973 by D.Ellott. Bell and Leanard J. LaPadula. It is a type of computer operating model used in the military sector. The mainly using of this model is to solve the confidential problem of access control. The subjects and objects of this model can be classified by their security mark, corresponding to the military security levels. It can effectively prevent information from a high-security level flowing to a low one. BLP model describes a military security strategy; for this reason, it is executed in a multilevel security field with strict security hierarchies. It has already got special attention from more of the researchers. As a hot research area in the multilevel security field, it has influenced the development of other security models a lot (Yanming et al., 2010; Sheng et al., 2010). The access

operation to sensitive information in this model has to follow up on these two concepts the ‘Least Privilege ‘and the ‘Need to know.‘

Figure 13: Bell-Lapadula confidential model (Source: Luke Ahmed, 2017)

2.7.1.2 The Biba model

Biba model was introduced in 1977 by K. J Biba. It was the first security model in the computer integrity field. It can be defined as a lattice-based access control security model dealing with multilevel sensitive information (Sandhu, 1993). The main idea of the Biba model is to applying information flow policy by using mandatory access control to strengthen discretionary access control. According to mandatory access control policies, it checks flows of system information to find and to prevent the possible destruction in the system. The subject and object in the Biba model have their integrity level. The higher-level data has higher accuracy and reliability than a lower one. Unlike the BLP model, the Biba model is used in the commercial applications. The integrity of data is more important than the confidentiality. It based on the integrity level, so it is used to solve the integrity problem of applications ‘data and its access control. The significance of the Biba model is to protect the integrity of the information system.

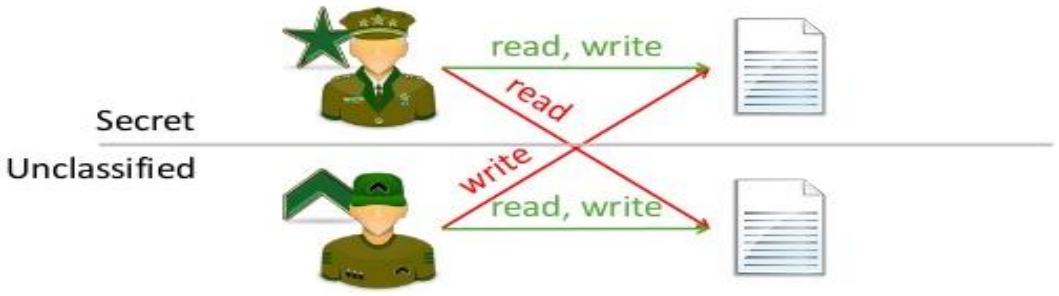

Figure 14: Biba integrity model (Source: Cybrary, n.d.)

2.7.1.3 Clark-Wilson model

Clark-Wilson model suggested in 1989 by David Clark and David Wilson; the Clark-Wilson model focuses on the integrity of information and system. In this model, an agent program is applied to access objects in order to protect the integrity of objects (Jing and Meihui, 2012). So, the user cannot directly access and control objects. The main idea of the Clark-Wilson model is to use the benign transaction processing technique and task separation technique to ensure the consistency of data and the integrity of the transaction. The good transaction processing technique means that the processing of information has to be restricted in certain privileges and ranges. The task separation technique divides a task into different task subsets. Every subset has to be done by at least two people. By this technique, personal bluffing can be prevented.

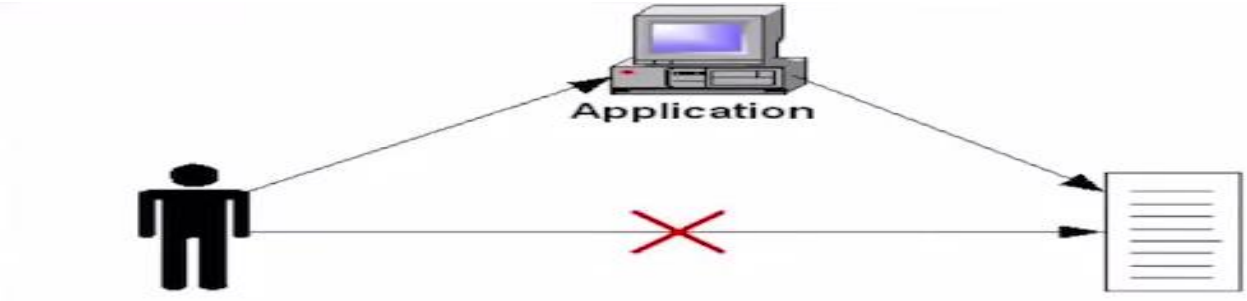

Figure 15: Clark-Wilson model(Source: Amoroso, 1994)

2.8 Comparison of security models

In this section, the comparison between the previous models focuses on Design Year, Aim, Rules, Specification, Limitations, Filed, and Advantages, as shown in Table 3.

2.8.1 Design Year

The first model is the BLP, which is designed in 1973. It is the most famous MLS model. The second is the Biba model which is

designed in 1977. The third is the Clark-Wilson model, which is published in 1987 and revised in 1989.

2.8.2 Filed

BLP model is a model that imitates the military security strategy. Clark-Wilson model imitates the business environment. The Biba model can be applied in a wide scope.

2.8.3 Specification

BLP and Biba models have strict formal languages, and Clark- Wilson model has informal languages.

2.9.4 Advantages

BLP model effectively prevents information from a high-security level flowing to low security because of its strict security classification. The Biba model is simple and can be combined with the BLP model. Clark-Wilson model can achieve all the three integrity protection goals.

2.8.5 Rules

BLP model rules are:

- Simple security rule (no read up)
- The property rule (no write down)
- Strong star property rule
- Subject with read/write – only at the same level.

Biba model rules are:

- Integrity axiom (no write up)
- Simple integrity axiom (no read down)

Clark-Wilson model rules are:

- Subjects and objects are labeled with programs.
- Programs hand out as an intermediate layer between subjects and objects.

2.8.6 Limitations

BLP model only focuses on the confidentiality of the information and ignores the integrity. On the opposite, Biba and Clark-Wilson models only protect integrity.

Table 3: Models comparison

Comparison	**Bell-LaPadula**	**Biba**	**Clark-Wilson**
Design Year	1973	1977	1989
Aim	Confidentiality	Integrity	Integrity
Filed	Military	Versatility	Business

Specification	Formal language	Formal language	Formal language
Advantages	Strict security classification	Simplicity and the combination possibility	Achieve three integrity protection
Rule	• Simple security rule (no read up) • The property rule (no write down) • Strong star property rule subject with read/write-only at the same level.	• Integrity axiom (no write up) • Simple integrity axiom (no read down)	• Subjects and objects are `labeled' with programs. • Act as an Intermediate between subjects and objects.
Limitation	No consideration of integrity	No consideration of confidentiality	No consideration of confidentiality

2.9 Previous studies on cloud computing in higher institution

Researches in higher institution relating to cloud computing over the last years are reviewed. This helps the researcher to identify the gaps in this area of research.

Alharthi et al. (2017) presented a framework for a successful migration to the cloud environment in Saudi universities and identified a set of critical success factors: technology, organization, legislation, and infrastructure. The results showed that the majority of these factors were statistically significant, except for the physical location factor. The proposed framework helps in decision-making while migrating to cloud computing.

In 2017, Shadreck Chitauro proposed the Cloud-Based E-Learning Implementation Model. This model should be used when one needs to make a technical decision on whether to implement a cloud solution or not. To use this model, the researcher proposes that one should consider all the components individually. The components in the Cloud-based e-learning implementation model are namely financial requirements, technical support, hardware and software requirements, and cloud computing security.

Another new e-learning framework based on private cloud and the virtual private network was proposed by Jayasena and Song (2017). The proposed framework helps students in the university environment to access the e-learning environment for resource sharing with less cost.

Ashtari and Eydgahi (2017) addressed the influence of individual users' perception of cloud computing applications. The researchers presented a framework focused have influenced the perceptions of cloud computing at the University of Southeast Michigan students. Additionally, the Technology Acceptance Model (TAM) model was used for analyzing the adoption of cloud computing by students. Although the usage of the TAM remains significant in technology evaluation after its adoption, there is a lack of any practical values and limited explanatory.

Arpaci (2017) also used the TAM model to investigate the antecedents and consequences of cloud computing adoption in higher education to achieve knowledge management through the questionnaire mode of data collection among undergraduate students in the Turkish university. The findings showed that educational institutions promote cloud computing adoption by increasing the awareness of knowledge management, although the research is limited to critical issues only.

Rahimah and Aziati (2017) studied the factors that affect the cloud computing implementation in HEIs, focusing on SaaS. The researchers projected a framework extracted from the Technology, Organization, and Environment (TOE) framework and integrated with the Diffusion of Innovation (DOI) theory for this study. Although the projected framework accelerates the implementation method of computing technology, it does not consider the individual's resources or social support to adopt the new behavior. The proposed framework focuses on flexibility, mobility, low cost, and business continuity. However, security, reliability, and loss of sensitive data were not considered in the research. Furthermore, there is a lack of standards to enable multiple clouds to work as a single entity.

Madhav and Joseph (2016) proposed a framework for cloud-based virtual computing labs in a higher institution in South Africa. The findings of this research show that higher institutions can save costs on hardware, software, and helps in the flexibility of the cloud-based virtual computing labs. However, this framework was demonstrated with one university.

Khan (2015) proposed a hybrid-computing model that facilitates Saudi Arabia's higher education institutions to share knowledge and different research activities. The proposed model focuses on improving the quality and effectiveness of teaching by providing support tools. Security issues were not considered in the proposed model.

A survey conducted by Alajmi and Sadiq (2016) demonstrates that cloud computing continues to play a progressively important role in teaching within the present time. However, there is a dialogue on totally different problems like privacy, integrity, and ownership of data. Moreover, there is an absence of the latest security techniques to adopt cloud computing within the universities.

Militaru et al. (2016) explored the factors that result in cloud computing adoption in pedagogy supported the tam-o'-shanter framework by measurement ninety-six students at a university in Roumania. Findings discovered that the factor's area unit essential to boost the understanding of cloud computing adoption for school members and students. However, there is a scarcity of any sensible worth and restricted instructive.

Another wildcat study supported the Technology Organization setting (TOE) framework conducted by Tashkandi and Al-Jabri (2015) aimed to spot the factors that affect cloud computing adoption by pedagogy establishments in Saudi Arabia. The factors were tested through applied math analysis, and also the results discovered the importance of the subsequent factors: quality, relative advantage, and information considerations. Although the researchers provided a higher understanding of things moving cloud computing adoption, they did not embrace information measure and dependableness factors in their study.

A case study conducted by Musungwini et al. (2016) this study proves the benefits of using Google Docs in academics and analyzed the factors affecting cloud computing adoption at a university in Zimbabwe. Interviews and questionnaires were used for data collection to get in-depth on the issues affecting cloud computing adoption. Findings revealed there are many benefits of Google Docs to academics, but there is also a lack of knowledge on how to use the technology among lecturers, although the researchers did consider the security issues of the system.

Ibrahim et al. (2015) review 27 papers to analyze the evidence of cloud computing adoption. The result clearly shows that security and privacy are some of the significant challenges of why the adoption rate is slow.

Pardeshi (2014) proposed a cloud- computing architecture for higher education institutes that contain cloud computing deployment models, services models, and user domains. Although the proposed architecture improves agility and increases efficiency, it has not yet been evaluated.

Akande and Belle (2014) explored SaaS to know if it is the best option for the education sector in South Africa. Interviews were conduction on undergraduate students regarding the use of Office 365 as SaaS. Findings revealed that Office 365, present so many advantages such as cost reduction, infrastructure maintenance.

Njeh, in 2014, studied several studies that were undertaken to establish factors that influence technology adoption. Njeh (2014), proffers that the most widely used is the technology acceptance model (TAM). Njeh (2014) criticizes the TAM by stating that it "does not address features of modern technology," and thus, Njeh (2014) introduced the Cloud Computing Adoption and Use Model. CCAUM is an improvement of TAM because it encompasses the TAM and TAM2, and it has been extended to include five additional categories of features that are namely; technology features, economic factors, security and privacy, standards, and control.

Table 4: Summary of related studies

Author(s)	**Technology**	**Pros**	**Cons**
Alharthi et al. (2017).	Framework	• Investigate factors affecting migration to cloud in South Africa. • Supports decision-making processes, whether to migrate or not. • Provides empirical data for cloud-computing projects.	• Not implemented.
Shadreck Chitauro (2017)	Model	• Cloud-Based E-Learning Implementation Model	• Security issues not considered.
Jayasena and Song (2017).	Framework	• Scalability. • Increases availability and reliability.	• Limited access within the campus.
Ashtari and Eydgahi (2017).	Framework	• Effective usage of the model.	• Lack of any practical values. • Limited explanatory.

Arpaci (2017).	Model	• Efficacy.	• Limited explanatory.
Rahimah and Aziati (2017)	Framework	• Accelerated technology implementation in HE.	• Individual's resources or social support did not consider.
Al-Hamami and Hashem (2016).	Framework	• Lower cost. • Flexibility. • Mobility. • Business continuity.	• Security issues not considered. • Reliability issues. • Loss of sensitive data. • Lack of standards to enable multiple clouds to work as a single entity.
Madhav and Joseph (2016).	Framework	• Software and hardware costs were minimal. • Flexibility.	• It only uses the framework within the campus.
Khan (2015).	Model	• Treasure of knowledge at one place. • Improves the effectiveness and quality of teaching. • Budget saving.	• Security issues not considered.
Alajmi and Sadiq (2016).	Survey	• Increases in productivity. • Penetration of knowledge. • Improves educational strategies.	• Integrity, privacy, security, and ownership of the data. • Lack of new security techniques.

Militaru et al. (2016).	Framework	• Effective framework.	• Lack of any practical values. • Limited explanatory.
Tashkandi and Al-Jabri (2015).	Framework	• It provides valuable insights into critical factors that affect the adoption of cloud computing.	• Lack of including bandwidth and reliability.
Segrelles and Molto (2016).	Platform	• Flexible platform.	• The complexity of communication among the levels.
Musungwini et al. (2016).	Case study	• Using different research design approaches. • Help in the collaboration process	• The security issue was not considered in the research.
Ibrahim et al. (2015).	Survey	• High quality selected research	• Non
Pardeshi (2014).	Architecture	• Improves agility. • Increases efficiency	• Lack in the evaluation stage.
Akande and Belle (2014).	Model	• Allow focusing on teaching and learning. • Reduces cost. • Improves access to resources.	• Using costly application.

2.10 Proposed secure cloud-based ERP model

The Proposed secure cloud-based ERP model. A security model is needed in cloud computing to coordinate scalability and multi-tenancy with the requirement for trust. Since cloud computing involves the pooling of resources so that multiple users can have access to them, data stored or managed in a cloud are likely to face security issues.

When higher institution moves to a cloud environment with their identities, information, and infrastructure, they must be willing to give up some level of control. The organization must trust

its cloud computing systems and providers, but still, be able to verify cloud processes and events. The fundamentals of trust and verification are access control, data security, compliance, and event management. Cloud computing services and mechanisms include authentication, authorization, data encryption, data privacy, and multi-tenancy. And cloud services and mechanisms. These requirements are mandatory to achieve integrity and coherence in cloud systems.

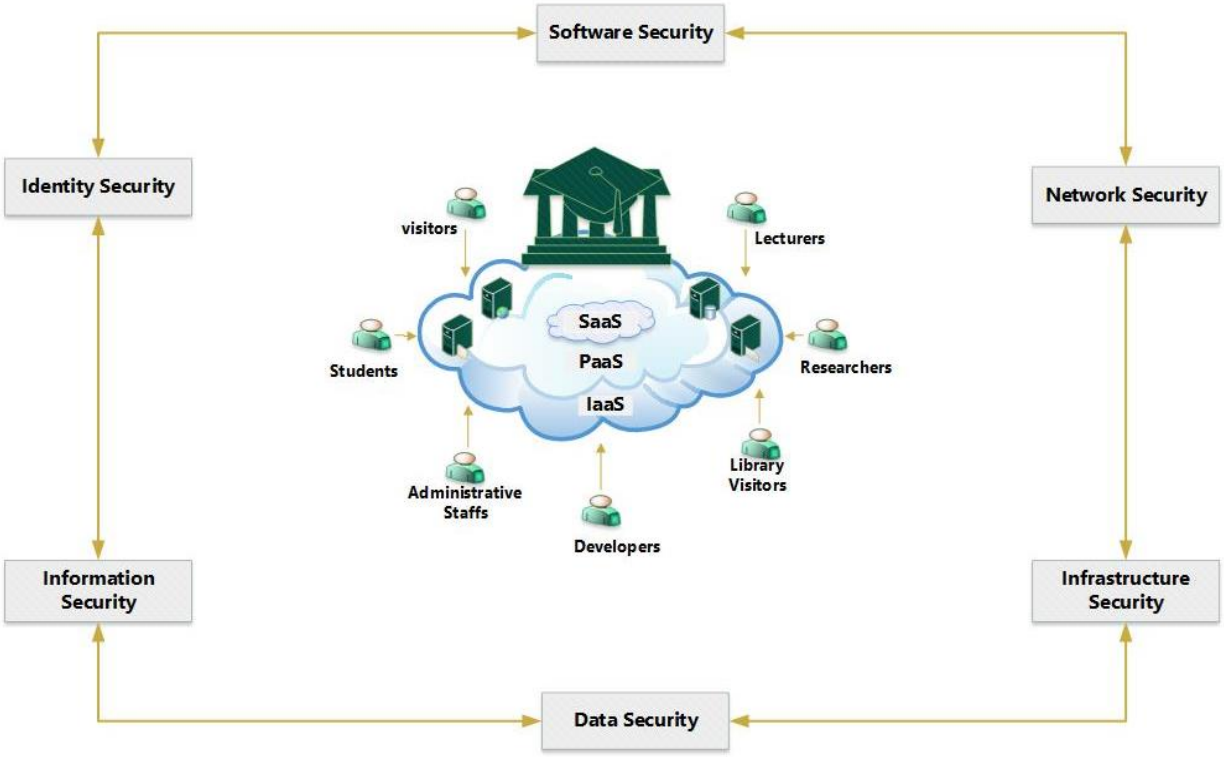

Figure 16: Proposed secure cloud-based ERP model

From the literature reviewed, the researcher put into consideration core security parameters, which are: the software security, hardware security, information security, identity security, network security, data security, and infrastructure security.

Identity Security: These will ensure the integrity and confidentiality of data and applications while increasing their accessibility to appropriate users. End-to-end identity management, third authentication services, and identity are crucial elements of identity security in the cloud. Management in identity security possesses capabilities that should be made available to both users and infrastructure components in cloud computing.

Information Security: Information security responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage. The controls on physical access, access to hardware and software, and identity controls are targeted towards the protection of data. The protective barrier in the cloud ensures the security of information is diffused.

Infrastructure Security: Demonstrating that the virtual and physical infrastructure of a cloud can be trusted is a challenge. The attestation of a trusted third party (TTP) is not sufficient for critical business processes. It is essential for an organization to be able to verify business requirements that the underlying infrastructure is secure.

Network Security: Network Security is an essential requirement for cloud computing. It involves taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users, and programs to perform their permitted critical functions within a secure environment.

Software Security. While there is a broad range of software development efforts in terms of scope and difficulty, all of them require assurances of security. Since there is no such concept as guaranteed full security, the goals are to create secure software with security carefully designed into it, not an after-thought add-on capability. In this way, it is possible to build software with a high degree of protection against attacks.

CHAPTER THREE

METHODOLOGY

3.0 Introduction

This chapter outlines the research methodology, data collection design, and setting of the study. The chapter also provides an insight into the research methods applied during the data collection, the tools, validity, and techniques used for data evaluation. There were two phases of data collection used for the study. The first phase involved a comprehensive case study analysis comprising four interviews with representatives from ICT department who manages the day to day activities of the server-based ERP system, followed by an online expert panel consisting of a broad range of domestic and international academic and professional in ERP developer, information security analyst experts. Both data collection phases were used to improve and refine the proposed model content and its presentation.

3.1 Research approaches & theoretical perspectives

In this study, an attempt is made to generalize (in the form of the model) from specific inputs received from the data collected. The research relies on an overall documented knowledge about server-based and cloud-based ERP and its security challenges while understanding its relevance to the higher institution.

3.1.1 Interpretive approach

An interpretive approach is associated with qualitative research (Williamson et al., 2002). Researchers normally start with an assumption and attempt to investigate or understand a problem via a social construct, such as language and the shared meanings people associate with the subject (King and Horrocks, 2010). Researchers conducting interpretive research mostly rely on natural settings in the area of interest and assume that there are differences between the social and natural worlds as the social world is constructed by people. This means that people develop their perspectives and interpretations of issues and consistently change their opinions (McNabb, 2012; Williamson et al., 2002). Furthermore, researchers initiate their study by gaining detailed insights on the topic from the literature and building strong theoretical foundations. The foundations for research include the theory, research questions, and establishing a data collection plan. The research might change or alter the research questions and the data collection mechanism if

unexpected, contrary views are raised about the topic. The researchers might not test hypotheses but develop working propositions that would be based on the research participants' opinions (Williamson et al., 2002).

3.1.2 Positivism and post-positivism

Two other commonly used research perspectives are positivism and post-positivism:

Positivist research is generally associated with quantitative data collection methods, such as surveys (Williamson et al., 2002). The post-positivist paradigm also involves qualitative research, such as interviews and focus groups (Denzin et al., 1994). Koch (2003) defined positivism as a certain set of interrelated assumptions in the social arena that provide a conceptual and philosophical framework. This is designed to create a systematic understanding of a study. It is generally understood that positivist research delivers results that could be measured or replicated. However, Silverman (2013) was of the view that the purpose of positivist research was not to produce scientific laws, but rather cumulative generalized understandings derived from tedious data analysis. Positivist research could also be associated with deductive reasoning that could further relate to a hypothesis testing approach. In this approach, a researcher could first establish a theoretical foundation and/or a model with defined variables to test. The researcher could forecast relationships by framing the hypothesis and testing them (Weideman, 2013; Williamson et al., 2002).

3.2 Research methods

There are several different methods that could be used to inform research, including grounded theory, action research, conversational analysis, life history, case study research analysis, etc. (Myers, 2002; Neuman, 2006). According to Leedy et al. (1997), "Methodology is merely an operational framework within which the data are placed so that their meaning may be seen more clearly." The research method applied to this study primarily focused on a case study for the first data collection phase staff and the second phase uses a modified Delphi method for the second data collection.

3.2.1 Phase one: Case study research approach

The case study method was employed for data collection in the first stage of this study. For this research, a case study refers to a specific form of investigation that requires an in-depth analysis

of a program, activity, or process (Stake, 1995). Similarly, Yin (2003) defined a case study as an empirical study that investigates a contemporary phenomenon in a real-life context, where the boundaries between the phenomenon and context are unclear. For effective and comparative data analysis, four staff from the ICT department at the case study (Kampala International University) were interviewed. The revised model from the first data collection stage (interviewees) was presented to the expert panel for discussion, and they commented based on their practical experience. According to Yin (2003), the case study analysis provides an enriched insight into data. It brings an understanding of inadequately understood phenomena in a real-world setting with the assistance of the transferability of research findings.

The researcher analyzed a particular case study restricted by the area of the context under investigation. This allows the researcher to obtain detailed insights via a diverse range of data collection procedures (Leedy, 1997). The collected data from an in-depth case analysis provides confidence in the findings, especially in the case study research (Miles and Huberman, 1994). Case study analysis have different data collection methods, such as those identified by Yin (2004) which include: documentation (written materials, publications, newspaper clippings); achieved records (organizational charts, financial records); interviews (formal or informal, open-ended or focused); direct observations (obtaining details, actions, environment; and examination of physical artefacts (devices, output tools). For this study, the researcher used data collection methods, including written implementation documents and formal interviews.

3.2.2 Phase two: A modified Delphi approach

Some researchers argue whether to classify the Delphi approach as a data collection technique or a research method (Williamson, 2002a). Some researchers questioned it to be both an art of science (Linstone and Turoff, 1975) and defined the Delphi method as a blend of communication processes that would allow participants to deliver their thoughts and views while analyzing a complex problem. In another view, the Delphi technique is seen as a platform to obtain comparability and discover opinions and consensus regarding topics in a discussion (Green, 1999; Baretta, 1996). It is designed to prompt discussion for the purpose of obtaining individual responses while enabling experts to refine their views as the discussion progresses (Adler, 1996). This approach also provides an opportunity to gain a better understanding of the issues and argue more effectively (Watson, 2008). Generally, participants in a discussion have a deep interest in the topic, bringing

valuable knowledge and/or experience to that discussion (Delbecq, 1975). Delphi's approach involves a series of 'rounds' of data collection. The model or concept being tested is revised at the end of each round. Rounds are conducted until there is agreement or differences cannot be resolved (Williamson, 2002a). This study was a modified Delphi as it did not involve regular rounds. Typically, there are two processes in the Delphi approach.

The first is known as the conventional method.

- This is moderated by an individual who designs the questionnaire and forwards it to a large group of experts participating in the discussion. The feedback is then analyzed, and another questionnaire is developed based on the feedback received.
- The second type of Delphi process is known as the real-time Delphi method. In this technique, the moderator is replaced by a computerized program, and participants in the discussion communicate through the internet, responding to an online questionnaire. In this method, a real-time communication system is used to eliminate any delay in summarizing results. It is also essential to have a robust selection for the expert panel and the approach for an active and continuing participation in the discussion (Watson, 2008).

In addition to the Delphi approach, according to Daneshkhah (2004), expert judgment is another method that can be used in qualitative research. This can be an informed assessment based on an expert's knowledge and experience relating to the quantity or quality of content in the discussion. The judgment could be considered as a process of gathering and establishing opinions about a research topic under investigation. There could be several criteria used to select experts for a research study. Including their experience, research, and publications in the area of research, positions, and awards received (Daneshkhah, 2004). It was further explained by Daneshkhah (2004) that expert judgment is applied when data is limited and difficult to obtain because of higher costs, unknown models, or data open for interpretation and feedback. These data problems are brought to the expert's attention for discussion.

For this study, in the second data collection stage, aspects of the Delphi approach were applied. An online and offline expert panel was established, moderated by the researcher. The researcher developed a list of questions based on the proposed model findings from the literature and posted them online for expert feedback. Based on the above definition of the Delphi approach by Watson

(2008), components of the real-time Delphi method were applied to establish a non-real-time online expert panel.

3.3 Data collection techniques

In the qualitative data collection and analysis framework, there are several techniques that can be used. From the list, only two techniques were employed relevant to the nature of this research study. The first data collection technique used was the case study interviews and the second expert panel.

3.3.1 Qualitative versus quantitative research

Qualitative and quantitative research techniques are employed by the researcher as they relate to their field of interest. Myers (2013) provided an explanation of the differences between qualitative and quantitative research methods as follows:

- Quantitative research was developed for the natural sciences to study natural phenomena. It includes research methods such as surveys, laboratory experiments, formal methods (econometrics), mathematical modeling, and so forth. Quantitative research relies heavily on numbers or numeric calculations.
- In contrast, the qualitative research method was developed in the social sciences to help researchers investigate social and cultural phenomena. Qualitative research includes action research, case study research, and grounded theory. The data sources for qualitative research include observations, interviews, questionnaires, documents, participant's perceptions (fieldwork), and the researcher's impression and/or reactions.

The qualitative research approach in this research, qualitative research techniques were applied. Qualitative research approaches help researchers understand people, social, and cultural experiences. According to Myers (2013). Further added that qualitative research is an optimal choice should the study be about an in-depth analysis of one or more organizations. This technique is suitable for exploratory research when the topic is new, and there is limited published research on the topic. It is also suitable for social, cultural, and political research analyses of people and organizations. According to Cleary (2014), qualitative research is conducted to collect information-driven generally from observations and interviews. It is conducted in a realistic setting with an interpretive nature. Qualitative analysis is used to answer questions about natural

phenomena for the purpose of describing and comprehending the phenomena from participants (Leedy et al., 1997). In other words, qualitative research focuses more on the social world rather than the world of nature. The social world is related to human beings and relies on the subjectivity of experiences (Liamputtong, 2000). From Malhotra's (2010) perspective, the qualitative research approach seeks a better and more precise understanding of the issues under investigation. From a broader perspective, qualitative research could be defined as:

A research method that allows the researcher to examine people's experiences in detail, by using a specific set of the research processes such as in-depth interviews, observation, visual methods, discussion, content analysis, focus group, and biographies or life histories, (Hennink et al., 2011). Cleary (2014) further alluded that before initiating qualitative research, it is fundamentally essential to complete a detailed analytical and critical literature review. This ensures that the researcher has an optimal understanding of the latest knowledge and perspectives on the area/field of interest. It also enables the researcher to clarify research questions, potentially shift the focus, help to extend the findings, and clarify perspectives. Silverman (2013) listed several vital points to remember about qualitative research, as follows:

- Qualitative research involves a variety of different approaches.
- A single common thread could attempt to make routine features of everyday life problems.
- Some qualitative research could be criticized for being insufficient, but the same could be said for some quantitative research.
- Always make a pragmatic choice between research methodologies under the research problem and the proposed model.
- Qualitative research should apply rigorous, critical standards.

It is argued that the disadvantage of qualitative research is that considerable population input cannot be generalized, and the data remains focused on a specific group of participants. In other words, a researcher could generalize from qualitative research but is unable to use sampling logic for generalizing purposes. For instance, if a research study is carried out on three case studies, the data sample size of the three cases would remain valid for those three and cannot be considered in statistical terms (Myers, 2013). For this research, the researcher adopted a qualitative research approach to get an in-depth analysis of the current server-based ERP system and to determine the

requirement for a secured cloud-based ERP. The first secure cloud-based ERP model was developed based on a comprehensive literature analysis and interview. The final revised version of the model was developed with an online and offline expert panel.

The reason for employing two qualitative data collection techniques the case study and expert panel and the case study analysis was to thoroughly test the proposed secure cloud-based ERP system. Other qualitative data collection techniques were not used as they were not appropriate for this study. One of the benefits of interviews, according to Williamson (2002c), is that they allow the researcher to control the direction of the discussion, enabling the use of quotes specific to the situation and ensuring that the interviewees remain focused on the topic in hand.

3.3.2 Phase One: Case study interviews

In the first stage of the study, a case study was conducted. Interviews are widely used by researchers in qualitative research (Barbour, 2008; Bryman, 2008). Liamputtong (2009b) viewed interviews as one-on-one or face-to-face interactions between participants and researchers, providing the interviewee's insights on a range of relevant topics. In this research study, the case study is Kampala International University, an in-depth one-to-one interview with four staff who manage the day to day the current server-based ERP System. According to Holstein and Gubrium et al., (2003), the interview approach is an empirical data collection process in which an individual is encouraged to provide views on certain aspects in detail. Williamson (2002) listed some advantages of the interview approach in qualitative research:

- Interviews enable researchers to gather in-depth insights on issues.
- Interviews enable researchers to get first-hand responses from participants.
- Interviews enable open communication and exchange of information.
- One-to-one interviews have better response rates than indirect communications (e.g., via mail or email).
- Questionnaires in interviews evolve due to one-to-one contact with interviewees.
- The interviewer can control the discussion and keep interviewees focused on the issues being discussed.
- Unstructured interviews can be more flexible and expand on essential aspects, as various issues are discussed.

Some interview disadvantages were highlighted by Malhotra (1999), as follows:

- The limited skills and capabilities of the interviewer can be an issue.
- Lack of structure could make the outcome vulnerable to the interviewer's influence on interviewees. This could result in quality being compromised.

Types of interviews

There are three types of interviews that could be considered for qualitative data analysis (Williamson, 2002c). These are:

- Structured interviews are standardized and/or scheduled before their inception. All interviewees are asked the same questions in the same pattern or sequence. There may be some freedom provided to interviewees while they express their opinions, thoughts, or views unrelated to the strict agenda followed by the researcher.
- Unstructured interviews are non-standardized, unscheduled, and in-depth interactions with interviewees. The interviewer follows the flow of discussion, and every interview answer could result in a new question. This type of interview is to gain new insights from interviewees and is appropriate for case studies to cooperative extensive data from key individuals. This type of interview is acceptable for interpretive research.
- Semi-structured interviews are based on a standard list of questions, but the interviewer could follow the lead of interviewees or ask them additional questions to seek more detailed responses. This type of interview is closer to the unstructured approach than the structured one.

For this research study, semi-structured interviews were used for the case study data collection. A list of questions was composed. However, due to the enormity of data sought, the interviewer remained open to discussion and allowed participants to share details as they considered them necessary or relevant. It is understood from the literature that the location of an interview could have an influence on the data being collected and the context of the interview, as this is considered to be a social interaction amongst two individuals (Neuman, 2005). Furthermore, it was suggested by Neuman (2005) that the interview should be conducted at a private or quiet location, such as a home. In this study, most of the interviews were conducted at the participants' office meeting

rooms, based on the availability of each participant. In two instances, interviews were conducted in the office, as suggested by participants due to their tight schedules.

According to Cavana (2001), there might be some non-verbal behavior issues that could impact on an interview. Some strategies and guidelines were suggested to counteract such behavior, such as:

- The interview pattern: clear patterns of interview interactions are required, by having excellent communication with interviewees through managing language barriers (if any) and encouraging participants to freely provide their insights and in-depth information.
- Listening: the feedback provided by participants in response to questions should be carefully comprehended, clearly interpreting the essence of the comments made.
- Paraphrasing: the interviewer must precisely paraphrase the valid message communicated by the interviewee.
- Probing: relevant questions should be asked to dig deeper and produce more in-depth insight into the relevant information.

All interviews were carefully planned, organized, and scheduled before their inception. A list of individuals who were relevant to the area of interest was made, and each individual was informally contacted and invited to participate in the study. As a result, some individuals declined, and some agreed to participate. Every potential participant was requested to provide a date, time, and venue for their liking to schedule an interview session. The consent information that outlined the purpose of this study and a statement that their participation would remain confidential was provided to each participant. The researcher was aware of the deficiencies of the interview process, such as bias, interviewer characteristics, and the effects of the interviewer on the discussion. To address these challenges, the researcher-maintained impartiality, remained focused on the topic content and professional throughout the interview process

Interview questions

The interview questions were developed within three categories or phases. In the first phase, standard organizational questions were asked to obtain an insight on the operation of the system, the second is on the challenges faced by the system, and the third is the requirements for a secure

ERP system. In some instances, interview questions were paraphrased differently to address the different characteristics, knowledge, and background of the interviewees (Manaster, 1972).

Recording interviews

During the interview process, it is difficult for a researcher to capture all details correctly; hence, recording the interview could be advantageous. The researcher may forget all the critical details of the interview should they decide not to record it appropriately (Flick, 2009). It is an ethical responsibility of the researcher to seek authorization or approval from the participant before the recording of the conversation could start. Should a participant refuse to be recorded and/or not be comfortable with the recording, this would be a challenge for the researcher and threaten to disrupt conversation (King and Horrocks, 2010).

For this research, the audio recording feature of the researcher's infinite mobile phone was used to record conversations. Also, the researcher took extensive written notes while conducting the interview and maintained a balanced approach to ensure that the interview followed a sequence and was not disrupted. At the start of each interview, participants were provided with a hardcopy of the questions along with the proposed model.

The interviewees were asked to provide feedback on the factors and were encouraged to add, delete, or move factors from a stage if they thought it necessary. The researcher immediately noted any changes to a hardcopy. The participants also assisted the researcher to write notes and provide clarification as deemed necessary.

3.3.3 Phase two: The expert panel

In the second phase of data collection, an online expert panel was established with experts from a wide variety of backgrounds associated with the topic of research. The discussion was conducted online and offline to enable flexibility for the participants, given the experts for discussion were selected from various locations around the world. It would have been impossible to have all experts in one location at the same time; consequently, the online expert panel provided an opportunity for an open interaction amongst experts, at their convenience, and discussion on every aspect of the model.

The offline expert panel was in the case study. This helps the researcher to get feedback from an academic expert in the area of cloud security. The participants were contacted informally first to obtain their consent to participate. Experts who agreed to participate in the discussion were later formally inducted to establish the expert panel. The expert panel discussion ran over one week, with a specific aspect of the topic covered each day. The comments and feedback received from experts were analyzed and used to revise the conceptual model developed from the literature review and case study. A consolidated view of the discussion was established, and the improved iteration of the model reflected the enhancements based on the expert panel discussion.

3.3.3.1 Selection of online and offline experts

For this research, it was essential to ensure diversity in selecting experts with a wide range of experience in both cloud computing, ERP, and information security domains. It is generally understood from the literature that even though best practice knowledge exists, it is often ignored. This causes ERP security failures (Tsai et al., 2012; Vandaie, 2008; Rao, 2000). It was important for this study to seek diverse opinions and a variety of feedback on the topic and the proposed model content. After an initial investigation into their suitability for this study, a total of 25 experts were contacted, but 12 responded, and 08 participated. Primarily, the selection criteria were based on the following:

Academic experts with teaching and/or research experience with cloud computing and information security. Research and teaching experience would be advantageous.

- Professional experts with project management experience and/or cloud ERP management experience and/or experience with cloud security.

The primary means used to contact these experts were as follows:

- Personal contacts: Experts who were personally known to the researcher included those with productive ERP management, and/or information security experience. The essential criteria used to select from the personal contacts included years of experience in the field of ERP management and professional exposure information security or the relevant areas of security.
- Professional contacts: Experts were also selected based on their professional knowledge and associations with the researcher. The essential criteria used to select from professional

contacts included years of experience in the field of cloud computing, expertise in information security, academic professionals from ERP education, and ERP project managers.

- Academic journal articles and conference papers: Some experts were selected from the latest research publications on cloud security issues, especially about higher institutions. It was essential to include academics in the study with active involvement in cloud computing and ERP research, to discuss the model structure and allow for peer review of its content.
- Academic contacts: The academic contacts were selected based on their project management methodology experience, the knowledge of ERP applications, cloud computing security, and the relevance of cloud ERP applications in higher institutions.

The research has attended professional training (Project Management Professional, Python for Security Professionals, Computer Hacking Forensics Analyst, WhiteHat Security Sentinel, and Ethical), which provide the researcher the opportunity to interact with a wide range of researchers and instructor and discuss the research topic. This enabled the researcher to establish some useful contacts that were later used to select experts in the area for this study. It was essential to obtain an academic perspective on the model findings so that the theoretical basis could be investigated.

- Academic contacts of the supervisor: Some of the academic contacts were suggested by the research supervisor. These were based on their contribution to academia, specifically in the areas of ERP management and application in higher essential.
- Professional networking site (www.linkedin.com): Finally, the professional networking website LinkedIn was used to attract experts in the area. A research brief was posted on different online forums: cloud ERP management, information security analyst, and cloud ERP platform developer forums. The posting contained an introductory message along with an invitation to indicate their willingness to participate in the study. It was also mentioned that the essential criterion needed to be met before an expert could be included in the study.

3.4 Ethical consideration

As this research required interaction with people and the handling of data obtained from the public domain, the researcher obtained the appropriate ethics approval from the University's postgraduate

department and was granted in June 2018. Venkatesh et al. (2011) define ethics as "a moral and legal right in conducting research." Andrew and Halcomb (2009) also say, "ethics is essential in the conduct of research and how research is always under scrutiny." There is a need to make sure succeeding issues are perceived while doing the research.

3.4.1 Obtain Consent

Participants will not be forced by the researcher to participate in the research, but consent will be sort before they can participate. The process is essential for the research to be successful. This research will not threaten the security of the participants in any way whatsoever.

3.4.2 Privacy and Confidentiality

It is the duty of the researcher to guarantee the confidentiality of the data that were provided by the participants during the research time and to make sure that the data are only used for the purpose if that particular research only. The respondents will remain protected as well as after the research study.

3.4.3 Deception

No participant will be forced to do anything without his/her consent since everything will be appropriately explained in detail so that the participants will participate knowingly.

3.5 Data analysis

According to Hennink et al. (2011), qualitative data analysis requires a valid interpretation of data using several different strategies. These are explored below.

3.5.1 Content analysis of the data

For the purpose of developing a model for this study, the content analysis could be considered as a useful method to test pre-existing findings or analyze data (Ezzy 2002). The content analysis related to different categories for data analysis and the categories define related aspects of the theory being tested. For the purpose of this study, the researcher let the categories develop from theoretical knowledge in the literature and later tested the data based on field knowledge using experts in the interviews and Expert Panel. This analysis enabled the researcher to have data emerge based on content for future analysis. In the first phase of the data analysis, the data was captured using interviews conducted with the experts in the area of interest. The content analysis was performed after all interviews were completed, and the data was extracted in transcripts from

each interview. Afterward, data collected from each interview was analyzed to identify common elements of the interviews. The content analysis for the second phase of data collection (the expert panel) was through obtaining expert comments and categorizing them by the critical components of the model. It is important to note that in qualitative research analysis, the researcher is likely to use other methods for analyzing the data that might be more sensitive to new categories and interpretations (Ezzy, 2002). Hence, for the purpose of this thesis, the researcher used content analysis as part of data analysis to identify the content within the data (Ezzy, 2002).

3.5.2 Interpreting data

To interpret the data, a few steps were followed in line with those suggested by Williamson (2002):

- Transcribe the data: The data was recorded for both data collection stages. This included an audio recording of interviews, recording notes, creating electronic documents to capture interview and expert panel details, and so forth. The recorded data was later transcribed and compared for consistency. This was to ensure that the information was accessible, allowing effective data management for later analysis.
- Go through all transcripts to familiarize: This is an essential step in data interpretation, and the researcher reads through all transcripts, notes, and other forms of data recording. This enabled the researcher to understand the data correctly and become familiar with the overall data before the analysis began.
- Create data categories: For the purpose of creating categories, the researcher used a code and retrieved process to understand the depth of data and comprehend the significance of some issues regarding the data. This was done by grouping data into several different categories and establishing relationships between each of those categories.
- Playing with ideas: A researcher can play with ideas at any given time. This enables the researcher to think about and consider data in different ways and gain a deeper understanding of its relativity and significance. For instance, common words, phrases, and ideas propagated by participants could be used by the researcher for the data analysis.
- Writing memos: A memo is a document that a researcher can create to illustrate ideas and information throughout the data collection process. This generally involves taking notes in the interview to transcribe the discussion.

- Conceptually organizing the categories: It is appropriate for the researcher to categories the data before conceptually organizing it. The initial categorization of data was completed based on the literature review and presented as the first iteration of the conceptual framework/model. It is also vital to continually organize the categories throughout the research process.
- Undertake word searches: Identification of common words or phrases that are frequently used is essential. In this study, a word search was not applied as, while the process is useful, it was not critical for the analysis.
- Form tentative theories: After completion of the previous steps, the researcher should write a statement and theories based on the data accumulated from the study. Practically, the researcher revised the conceptual framework based on each data collection process.
- Ask questions and check hunches: The final step in the process is to validate the statements and theories and the feasibility of the study before compiling the final report. The researcher should check references and supporting evidence for the statements, theories, and any evidence that suggests the contrary theme.

For this study, the changes made in the model were based on the data that had been gathered.

3.6 Validity and generalizability

To ensure quality in the research findings, there are two approaches; validity and generalizability (Gibbs, 2007) are discussed below.

3.6.1 Validity

Validity means the accuracy of research findings. According to Maxwell (2002), validity has been debated amongst scholars about the legitimacy of the qualitative research study. It relates to the consistency of results, policies, and programs or predictions. If qualitative research does not comply with such consistency, then the reliability of findings would be an issue. Maxwell (2002) also suggested that validity pertains to data, conclusion, and analysis, completed by a method with a particular context for a purpose. There are several ways to deal with validity challenges, both in qualitative and quantitative research. Researchers using quantitative methods, in contrast to qualitative researchers, generally deal with expected and unexpected risks to the validity of findings. For instance, Maxwell (2005) argued that qualitative researchers rarely have the benefit

of planned comparisons or strategies for sampling or statistical data manipulations. Consequently, researchers should rule out validity threats after research initiation by establishing alternative hypotheses for the evidence collected.

Two significant risks to validity were identified (Maxwell, 2005), and they commonly relate to qualitative research techniques. These are:

- Researcher bias: this takes place when data is selected based on the researcher's existing theory or research interests.
- Reactivity: this is the influence a researcher could have relating to the setting or individual studies.

Maxwell (2005) further argued that procedures or methods do not ensure validity, yet they are essential to mitigate the potential risks associated with validity and increase the credibility of results. For this study, the researcher used secondary data (literature), a case study, and an online/offline expert panel to support the validity of results.

3.6.2 Generalizability

Qualitative research does not usually allow a systematic generalization to a broader populace, in contrary to quantitative or experimental studies. Generalizability is defined by Maxwell (2002) as the extent or a level to which one expands the account/finding to another person, time, or setting beyond the actual account studied (Maxwell, 2002). According to Yin (2014), generalizability is often based on theoretical assumptions that lead to simplifying similar situations and the drawing of conclusions. It is recognized that sampling is essential for a researcher to establish interfaces from facts based on the person, event, or activity observed at first instance against the other facts, event, situation, and/or people at later times (Maxwell 2002). It is generally unrealistic to expect that a researcher would observe all aspects of a research study at a given time with the same setting concerning the study.

Maxwell (2002) highlights two aspects of generalizability, as follows;

- Internal generalizability: This includes generalizing within the setting, community, group, or institution studied as part of research to the person, event, or setting that was not directly included or involved.

- External generalizability: This includes generalizing beyond the group, context, or time that was not studied directly in research.

For this thesis and research study, both types of generalization were considered. The researcher is not claiming that the outcome of this research will apply to all cases discussed; however, this study provides an opportunity for the reader to make judgments on the applicability of the findings. The researcher does believe that as the model was extensively tested using qualitative data analysis techniques (case study interviews and the expert panel), elements of the model will be useful for migrating and implementing a secure cloud-based ERP in higher institutions. As data were collected from experts around the world, it is assumed that the elements of the model or findings would be beneficial or applicable for the higher institution in other countries as well. It is reported in the literature (Schofield, 2002) that case study analysis or a multiple case study approach could increase the generalizability of qualitative research. This research technique was used in the first phase of this study, but the data was only collected at Kampala International University in Uganda.

3.7 Design science processes

The cloud base secure model was developed and validated using design science. According to Hevner, Ram, March, and Park (2004), the design science paradigm solve problems that can be characterized by a critical dependence upon human cognitive abilities (e.g., creativity) to produce effective solutions. In this case, the problem at hand required the researcher to create a solution for security challenges that the higher institution was experiencing. Design science research proposes seven guidelines for use when solving a research problem (Hevner et al., 2004). The seven guidelines are:

1. Design as an artifact - Design science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
2. Problem relevance - The objective of design-science research is to develop a secure cloud-based model to essential and relevant higher institution problems.
3. Design evaluation - The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
4. Research contributions - Effective design science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.

5. Research rigor - Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
6. Design as a search process - The search for an active artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
7. Communication of research - Design science research must be presented effectively to both technology-oriented and management-oriented audiences.

In the case of this research:

i. A model was designed.
ii. The security and privacy-based model was aimed to solve the higher institution challenges presented by server-based ERP.
iii. The model only considers security and privacy aspects
iv. The design process encompassed expert panel and literature review, findings of the research, engagement of stakeholders, experiments, benchmarking with other models, and components identification.
v. Extensive research was done on the subject of cloud computing and ERP challenges, as shown in Chapter 2.

The steps that were followed, as shown in the figure below:

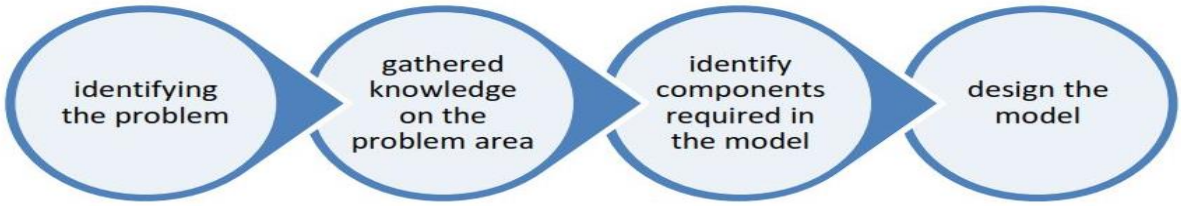

Figure 17: Steps to design the cloud-based ERP security and privacy model (Hevner et al., 2004)

The Cloud-Based ERP security and privacy Model depicted in the figure below is the proposed model that can be used when migrating from server-based to cloud-based enterprise resource system in higher institutions

In a distributed architecture it is necessary to adopt a security and privacy model to mitigate information security and privacy problems in higher institution; The base models considered for adoption in a security model are based on the BiBa and Bell-Lapadula model, since their merged features offer a model with integrity, confidentiality, and authenticity; which can be considered as an alternative to improve the security of information.

To mitigate threat problems, information security vulnerabilities in a distributed architecture, security policies, security models, rules, protocols, and appropriate security algorithms must be defined. It is concluded that it is necessary to have an adequate security model that adjusts to the operational, tactical, and strategic objectives of the higher institution to improve the confidentiality, integrity, and authenticity of the information.

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS, AND DISCUSSION

4.0 Introduction

The purpose of the research is to develop a secure model for cloud-based ERP system for higher intuition. This chapter aims to present and analyze the information collected through the data collection phase and deliberate on the data. A qualitative study engaging a multi-research site case study methodology was accompanied by data collected from interviews, expert panel, and document collection. Findings presented helped to respond to the following research question:

4.1 To study the current server-based ERP system used in a higher institution

To collect the data about current server-based ERP systems, semi-structured interviews were used. The following people were interviewed; ICT Director, software systems analyst, network administrator, and hardware systems analyst. These people were selected based on their roles as technical implementers and administrators of the current ERP system.

4.1.1 Discussion of interview results

From the interviews carried out the participants thinks it is a good idea to replace On-Premises ERP system with the one which is cloud-based because on-premises ERP system has many problems since all the participants tick all the five problems suggested: unauthorized access, denial of service (DoS), system viruses, breach of security policies and ERP system abuse by users. Unauthorized access is whereby the user accesses the ERP system without permission and considering the On-Premises system cost of servers, security issues, and employ qualified security personnel to guard data; the cloud is the option. From the interview conducted, it was established that higher institution is faced with two types of security challenges which is categorized under two main categories, i.e. security and privacy challenges:

Security challenges like Account and service hijacking, Malicious insiders, Authentication mechanism, Privileged user access, Browser security were the biggest worries of the higher institution which need to be addressed.

Privacy challenges like Data redundancy, Data loss, Data location, Data recovery, Data Privacy, Data Protection, and Data availability

These help the researcher to come up with the second model of the secure cloud-based model putting into consideration security and privacy.

4.2 To develop a security and privacy model for cloud-based ERP

This section focuses on the actual processes followed when developing the secure cloud-based ERP model. The actual components included in the model were derived mainly from the analysis of the results from the interview.

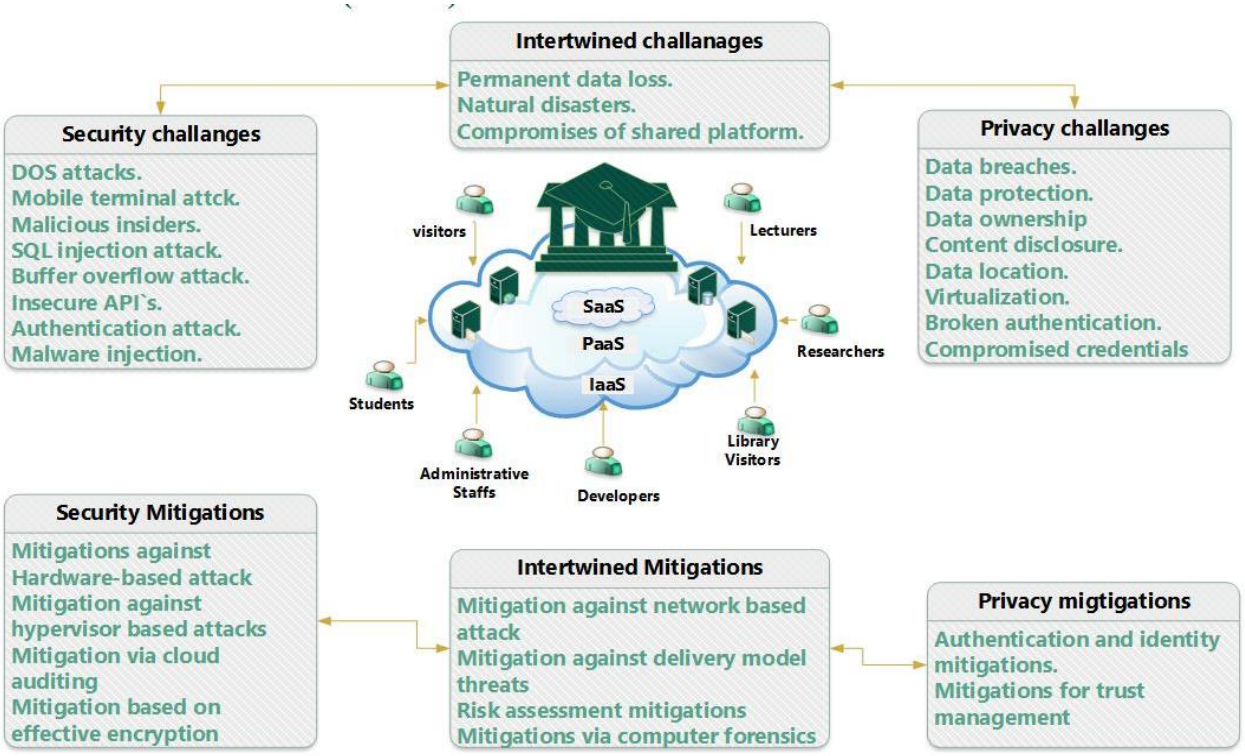

Figure 18: Secure cloud-based ERP model

Deciding on whether to implement a cloud or not is also influenced by the security provided by the cloud service provider. This was shown in the analysis of the results as well as in the prototype carried out where it was not possible to start using the cloud without setting up security parameters. From the findings, it was also clear that when a higher institution decides to migrate, they are not confident about cloud security. Therefore, when an organization decides to implement a cloud, they need to do a check on the available security options to make sure that they will suit their requirements. To enforce the security requirements, they must draft a security policy that clearly outlines the security services required from the cloud service provider, and this must be enforced

by making sure that the specifications required are part of the SLA. They must also make sure that the cloud service provider supports cloud security standards so that they can transition from one service provider to another, and it makes it easier for them to integrate security technologies with the cloud service provider.

4.3 To validate the developed security and privacy model for cloud-based ERP

This section focuses on the validation of the secure cloud-based ERP model using the design science process, stated in chapter three. The actual components included in the model were derived mainly from the analysis of the results from the expert panel. The validated secure cloud-based ERP model is presented below. The researcher contacted an initial investigation into expert panel members suitability for this study, a total of 25 experts were contacted, but 12 responded, and 08 participated. Primarily, and Appendix B shows the consent letter sent to the expert panel, and the model developed model was sent the them for their professional input and to help validate the security and privacy model.

4.3.1 Discussion of the expert panel results

From the expert panel, To enforce the security requirements, they must draft a security policy that clearly outlines the security services required from the cloud service provider, and this must be enforced by making sure that the specifications required are part of the SLA. They must also make sure that the cloud service provider supports cloud security standards so that they can transition from one service provider to another, and it makes it easier for them to integrate security technologies with the cloud service provider.

The expert panel suggested that it is better to put all parameters into consideration (security and privacy) when developing the model and removing the software and platform as a service model from the developed model Infrasture as a service should be adopted since these will help the higher institution to control their data/information.

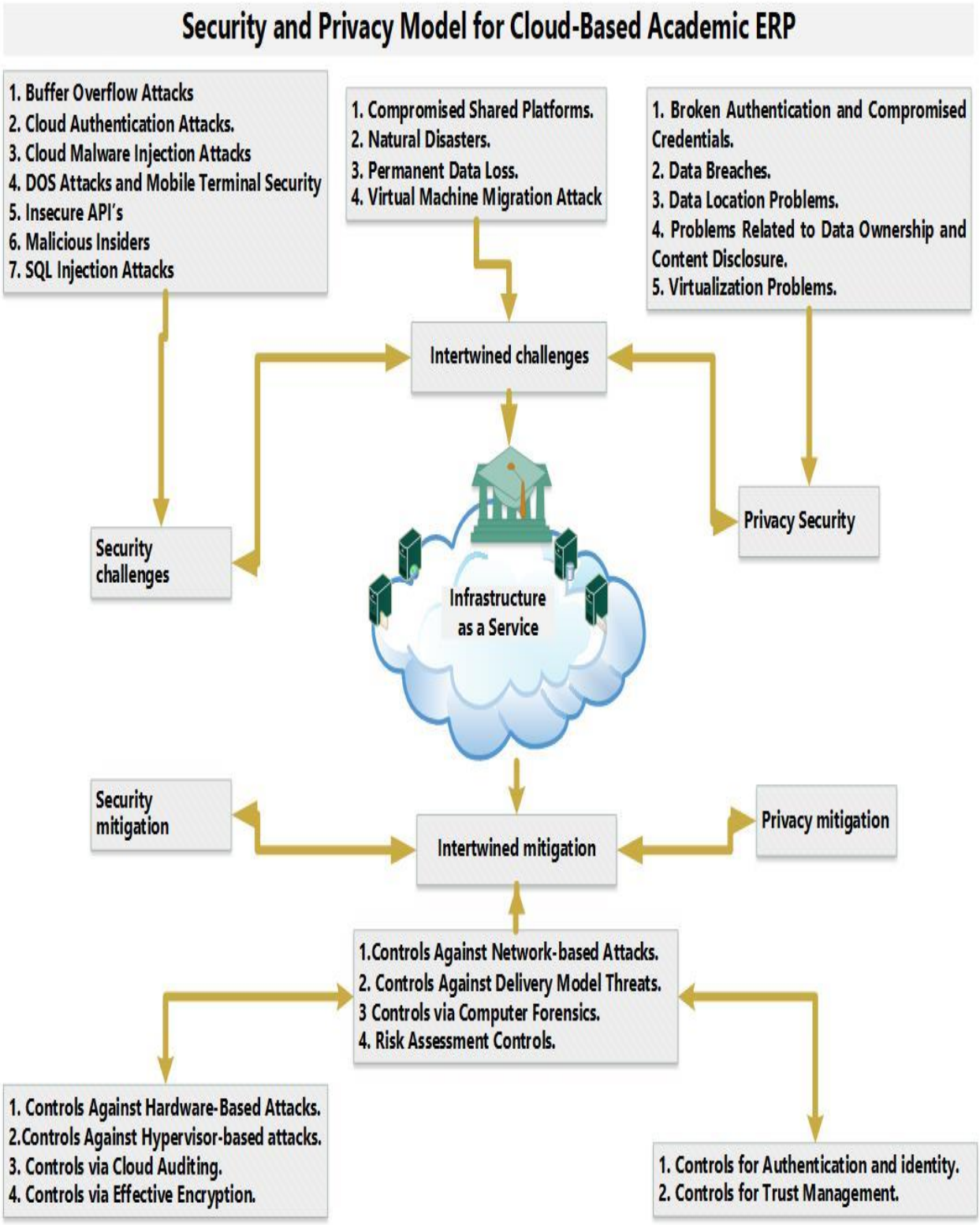

Figure 19: Validate Cloud-based security and privacy model

CHAPTER FIVE

RESEARCH SUMMARY, RECOMMENDATIONS, AND CONCLUSION

5.0 Introduction

This chapter highlights how the research objectives were met and the answers to the research questions. The research findings are also outlined in this chapter. Also, this chapter gives an account of how the research process was conducted and, finally, an account of which direction future research should follow.

5.1 Research Objectives and Results

The general objective of this study is to enhance security and consistency in cloud-based enterprise resource planning in higher institutions. To achieve this objective, the following sub-objectives were undertaken, namely to:

1. To study the current server-based ERP system used in a higher institution.
2. To develop a security and privacy model for cloud-based ERP.
3. To test the developed model.

The following sections will discuss how the objectives were met.

5.1.1 Main Objective

The researcher addressed this objective by designing a security and privacy model for cloud-based academic enterprise resource planning (CAERP). The model which was designed using the design research science can enable users of the model to identify that there is a need to migrate from server-based to cloud-based ERP without getting worried about security and privacy in the cloud. By following this model, higher institutions should be able to conclude that the current server-based ERP is not the adequate, and higher institutions should migrate to the cloud-based solution in order to gain from the benefits presented by cloud computing, which are discussed in chapter 2.

5.1.2 To study the current server-based ERP system used in a higher institution.

In order to come up with a practical solution, it was essential to determine the challenges that current server-based ERP platforms face. To determine what these challenges are, literature reviews were conducted, and interviews of experts that are currently administering the server-

based ERP system at this higher institution were conducted. From both these methods, it was established that the current server-based ERP system faces security and privacy challenges. Security and privacy challenges are situation where hackers, break into the network to alter information/data which is against the CIA principles of information security by altering students result, deleting of information/date, performing denial of service, injecting virus script in email/social media site and injecting trojan malware taking over the administrative staff computer to intersect information which give the hacker to hijack/copy/intersect confidential documents. Financial challenges are in the form of buying and maintaining site infrastructure, paying site licenses and individual packages and paying support staff. Awareness, confidence, culture, leadership, and motivation are the individual challenges in server-based ERP systems. Knowledge management challenges were outlined as content issues, copyright issues and the lack of an ERP strategy. Lack of technical support was also identified as an ERP challenge. It was established that ICT support skills are not adequate; there is a lack of ICT support skills that are required and support staff not being available. The final server-based ERP challenge which was determined is technological. This implies that there are infrastructural issues, resource management issues, bandwidth issues, power issues, and technical skills issues.

5.1.3 To develop a security and privacy model for cloud-based academic enterprise resource planning (CAERP) for Kampala International University.

The security and privacy model that is presented in this thesis should work in instances where one only considers the security and privacy aspects to decide to migrates to cloud-based ERP systems. Considerations of the model by the higher academic institution would yield the proper direction to follow, but as was revealed by literature reviews and interview findings, server-based ERP systems are not only affected by security and privacy challenges. They also face financial, technological challenges, individual, knowledge management, and support challenges.

The researcher believes that all these other challenges must be addressed in order to implement a fully capable cloud-based ERP system. Thus, even though it was revealed that migrating to cloud-based solutions would only solve security, privacy, financial, and technical ERP system challenges, there needs to be a way of solving all the challenges and incorporating them into the decision for cloud migration. The study also recommends that to protect data privacy when dealing

with the cloud, Data Encryption and Data Tokenization should be used when storing data in the cloud.

5.2 Recommendation

The Study recommends that higher institution should migrate to cloud-based ERP, this will help in: Reducing total cost of ownership, increase flexibility in IT implementation, Competitiveness, reduce security risk, improve privacy issues will also be solved and Time to archive objective

The study recommends that higher institution who have moved to the cloud should comply with the ISO27002 security standard, i.e. by limiting the data higher institution collect over the cloud, from the published report by ISO27002 higher institution should limit the use of the PII (Personal Identifiable Information) over public network, which higher institution should also set policies for retention and destruction of data after been collected, importantly know where your data is stored and make someone accountable.

The study recommends that Infrastructure as a Service (IaaS) should be adopted since higher institutions are concern with security and privacy of data in the cloud, but with the IaaS model both service providers and the client have roles to play in securing the ERP system.

it is also recommended that higher institutions should implement Simple and complex security strategy should be implemented, and this is possible if IaaS is implemented. A community cloud should be adopted, which understands its client needs.

5.3 Recommendations for future research

The CIA triad was mentioned above as the classic definition of security, or, being more precise, the classic definition of security services. However, there are more security services that are essential. Seven of them are provided as the standard set of security services by the International Standards Organization (ISO) (L. Lilien et al., 2017 and Al-Hassan et al., 2010). Similarly, privacy can be defined via a set of privacy services.

In the future, after identifying privacy services (analogously to the ISO's seven security services), all security and privacy issues (problems and solutions) could be categorized via a two-level classification. At the top level, we would still have the presented categorization into three classes: security-only, privacy-only, and intertwined.

On the second level, we would further categorize each top-level class into service-oriented subclasses. This means that the security-only class would be divided into (seven) security-service-based subclasses, the privacy-only class would be divided into privacy-service-based subclasses, and the intertwined-security-and-privacy class would be divided into intertwined-security-and-privacy-service-based subclasses.

This researcher focused on security and privacy in the cloud, also on how to successfully migrate from server-based ERP to cloud-based ERP using the Laravel framework platform for demonstration purposes. This can be further implemented on a live service provider server.

The content scope can also be explored by looking at Cyberlaw and policy, which guide both the cloud service provider and the client.

The geographical scope can also be extended by using multiple case study in the research in a higher institution; this can also be extending by using more than one university

5.4 Research conclusion

Cloud computing is a paradigm of computing that offers many valuable services to end-users, including processing, storage, and data management. However, it brings many security and privacy problems that require to be self-addressed. The security and privacy model was developed to assist higher institutions in Implementing of migrating to cloud-based ERP systems. Cloud-based ERP systems help the higher institution to provide a secure environment, costs in terms of hardware, software, and upgrades, as well as reduce up-front expenses.

The higher institution should enlighten/educate staff and students on Cloud computing awareness, its security challenges, mitigation and should be made mandatory for them to appreciate the importance of utilizing cloud computing in improving performance.

The higher institution should provide a reliable power supply system (Solar and UPS), increase internet bandwidth adequately, and the time to enable good respond time of the cloud-based ERP.

The volume of data produced by academic institutions grows every day. Due to the increasing numbers of staff, students, departments, and programs, this continuous growth requires continuous scaling and improvement of the academic ERP system. Therefore, to adapt to this continuous growth, the system should be constructed based on a cloud computing platform. Cloud-based

Enterprise Resource Planning system address many security and privacy issues in higher institutions: the increase of data/information, cost of hardware/software, data alteration, loss of data during migration from one server to another server, limited teaching materials and resources, high administrative costs, difficulties in managing large population of learners against small number of lecturers.

In this study, the researcher used a qualitative research design to examine the current server-based ERP system for Kampala International University and descriptive design to determine the requirements for the development of a secure model for cloud-based ERP system, which was guided by a well-structured interview guide and expert panel. Data was collected from the ICT department, interviewing four staff who manage the current server-based ERP system.

The findings from this study showed that higher institution is faced with security and privacy challenges that compromise the Confidentiality, Integrity, and Availability of data/information. Also, a security and privacy model was developed, which was guided by the findings from the analysis of the face to face interview, the expert panel conducted as well as literature reviewed. It is recommended that higher institution should migrate to cloud computing, Infrastructure as a Service (IaaS) should be adopted since higher institution are concerned with security and privacy issues in the cloud, Data Encryption and Tokenization should be used when storing data/information in the cloud and also comply with the ISO27002 security standard after migrating to the cloud. Hence, it is undeniable that a cloud-based ERP system provides a secure environment, reduces costs in terms of hardware, software, upgrades, up-front expenses, and promotes mobile computing, which is the ability to access resources from anyplace at any time.

REFERENCES

Alajmi Q and A. Sadiq, "What should be done to achieve greater use of cloud computing by higher education institutions," in 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016, pp. 1–5.

Akande A.O and J. P. V. Belle, "Cloud computing in higher education: A snapshot of software as a service," in 2014 IEEE 6th International Conference on Adaptive Science Technology (ICAST), 2014, pp. 1–5.

Alharthi A, M. O. Alassafi, R. J. Walters, and G. B. Wills, 2017 "An exploratory study for investigating the critical success factors for cloud migration in the Saudi Arabian higher education context," Telematics. Inform., vol. 34, no. 2, pp. 664–678, May 2017.

Arpaci I, "Antecedents and consequences of cloud computing adoption in education to achieve knowledge management," Computer-Human Behavior, vol. 70, pp. 382–390, May 2017.

AL-Hamami H.H and S. H. Hashem, "Sustainable Development: Proposing Cloud Computing Framework for Higher Education Ministry (HEM) in Iraq," Int. J. Adv. Stud. Computer Science Engineering, Gothenbg., vol. 5, no. 11, pp. 156–163, 2016.

AlCattan, R. F. (2014). Integration of cloud computing and network collaboration technologies in

Almishal, A., & Youssef, A. E. (2014). Cloud service providers: A comparative study. International Journal of Computer Applications & Information Technology, 5(2), 46-52.

Androcec, D. (2013). Data portability among providers of the platform as a service. The Journal of Slovak University of Technology, 21, 7-11.

Ashtari, S., & Eydgahi, A. (2017). Student perceptions of cloud computing effectiveness in instruction. Paper presented at the 2015 IEEE 18th International Conference on Computational Science and Engineering, Porto, Portugal.

Alharthi, A., Yahya, F., Walters, R. J., & Wills, G. (2015). An overview of cloud services adoption challenges in higher education institutions. Paper presented at the 2nd International Workshop on Emerging Software as a Service and Analytics, Lisbon, Portugal.

Alsufyani, R., Safdari, F., & Chang, V. (2015). Migration of cloud services and deliveries to higher education. Paper presented at the 2nd International Workshop on Emerging Software as a Service and Analytics, Lisbon, Portugal.

Ambrose, P., & Chiravuri, A. (2010). An empirical investigation of cloud computing for personal use. Paper presented at the 5th Midwest Association for Information Systems Conference, Moorhead, Minnesota, USA.

Alghali, M., & Roesnita, I. (2014). Challenges and benefits of implementing cloud-based e-Learning in developing countries. Proceeding of the Social Sciences Research ICSSR, 9–10.

Amoroso, E. G. (1994). Fundamentals of computer security technology. PTR Prentice Hall. Retrieved from http://www.softpanorama.org/Access_control/Security_models/clark_wilson.shtml

Adler, M., and Ziglio, E. (1996). Gazing into the Oracle: The Delphi method and its application to social policy and public health. Jessica Kingsley Publishers, Bristol, Pennsylvania.

Alzaid, E. A. J., & Albazzaz, E. J. M. (2013). Cloud computing: An overview. International Journal of Advanced Research in Computer and Communication Engineering, 2(9), 3522-3525.

Andrew, S., & Halcomb, E. (2009). Mixed methods research for nursing and the health sciences. UK: Blackwell Publishing Ltd.

Al - Shqeerat, K. H., A Al - Shrouf, F. M., Hassan, M. R., & - Jordan Hassen Fajraoui, A. (2017). Cloud Computing Security Challenges in Higher Educational Institutions - A Survey. International Journal of Computer Applications, 161(6), 975–8887. https://doi.org/10.5120/ijca2017913217

Badie, N., Hussin, A. R. C. & Dahlan, H. M. (2014). Cloud computing adoption factors for university administration. Jurnal Teknologi, 70(5), 81–87.

Baker, E. W., Al-Gahtani, S., & Hubona, G. S. (2011). Cultural impacts on acceptance and adoption of information technology in a developing country. Journal of Global Information Management, 3(18), 35-58.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599-616.

Benton, D., & Negm, W. (2010). Banking on the cloud. Retrieved April 20, 2018, from https://www.finextra.com/finextradownloads/featuredocs/accenture_banking_cloud_computing.pdf

Barbour, R. S. (2008). Introducing qualitative research: a student's guide to the craft of doing qualitative research (1st Edition ed.): Thousand Oaks, CA: Sage Publications Ltd.

Baretta, R. (1996). A critical review of the Delphi technique. Nurse Researcher, 3(4), 79-89.

Bryman, A. (2008). Social research methods (3rd Edition ed.). Oxford University Press; New York.

Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud computing: A study of infrastructure as a service (IAAS). International Journal of Engineering and Information Technology,2(1), 60-63.

Bhatiasevi, V., & Naglis, M. (2016). Investigating the structural relationship for the determinants of cloud computing adoption in education. Education and Information Technologies, 1-27.

Brohi, S. N., & Bamiah, M. A. (2011). Challenges and benefits of adopting the paradigm of cloud computing. International Journal of Advanced Engineering Sciences and Technologies, 8(2), 286-290.

Brodkin, J. (2008). Seven cloud-computing security risks. Retrieved September 12, 2018, from http://www.infoworld.com/d/security-central/gartner- seven-cloud- computing-security-risks-853.

Bell D.E and L. J. Lapadula, Secure computer systems, Technical Report, USA, 1973.

Chang, V., Wills, G., & De Roure, D. (2010). A review of cloud business models and sustainability. Paper presented at the 2010 IEEE 3rd International Conference on Cloud Computing, Miami, Florida, USA.

CCIA (2009). Abstract: Cloud Computing, Computer & Communications Industry Association. Retrieved on August 30, 2018 from HTTP:// www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/000000000151/Cloud_Computing.pdf

CDW. (2011). From tactic to strategy: The CDW-G 2011 cloud computing tracking poll. Retrieved from https://www.missioncriticalmagazine.com/ext/resources/MC/Home/Files/PDFs/WP_CWG_2011_Cloud_Computing.pdf

Cavana, R. Y., Delahaye, B. L., and Sekaran, U. (2001). Applied Business Research: Qualitative and Quantitative Methods. New York, U.S.A: John Wiley & Sons Inc.

Cleary, M., Horsfall, J., & Hayter, M. (2014). Qualitative research: quality results? Journal of Advanced Nursing.

Carpathia. (2015). Carpathia launches the healthcare community cloud service™ (HCCS™) beta program. Retrieved January 14, 2018, from http://carpathia.com/about/media/press-releases/Carpathia-launches-healthcare-community-cloud-service-(hccs)-beta-program

Chandra, D. G., & Borah, M. D. (2012). Cost-benefit analysis of cloud computing in education. Paper presented at the 2012 International Conference on Computing, Communication, and Applications, Dindigul, Tamilnadu, India.

Cybrary. (n.d.). The Biba and Clark-Wilson Integrity Models - Cybrary. Retrieved June 8, 2019, from https://www.cybrary.it/study-guides/cissp/the-biba-and-clark-wilson-integrity-models/

Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: Issues and challenges. Paper presented at the 24th IEEE International Conference on Advanced Information Networking and Applications, Perth, Australia.

Dye, M. A., McDonald, R., & Rufi, A. W. (2008). Network Fundamentals, CCNA exploration companion guide. USA: Cisco Press.

Davison, R. (2002). Technical opinion: Cultural complications of ERP. Communications of the ACM, 45(7) 109-111.

Delbecq, A. L., Vande Ven, A. H., and Gustafson, D. H. (1975). Group techniques for program planning: a guide to nominal group and Delphi processes. Scott Foresman, Glenview, Ill.

Denzin, Norman. K, Lincoln, & S, Y. (1994). Handbook of Qualitative Research. Thousand Oaks, CA, US: Sage Publications Inc.

Daneshkhah, A. R. (2004). Uncertainty in Probabilistic Risk Assessment: A Review. Unpublished BEEP working paper, University of Sheffield.

Ezzy, D. (2002). Qualitative Analysis: Practice and Innovation. Australia: Allen & Unwin.

Furht, B. (2010). Cloud computing fundamentals. In B. Furht & A. Escalante (Eds.), Handbook of Cloud Computing (pp. 3-19). New York: Springer.

Flick, U. (2009). An Introduction to Qualitative Research (4th ed.). London: SAGE Publications.

Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). Cloud computing and grid computing 360- degree compared. Paper presented at the 2008 Grid Computing Environments Workshop, Texas, USA.

Gilani Z, A. Salam, and S. Ul Haq, "Deploying and managing a cloud infrastructure: real-world skills for the CompTIA cloud+ certification and beyond," Wiley, Jan. 2015.

Girdhar, S. (2010). A walk in the cloud. Retrieved March 20, 2018, from http://smart-cloud-computing.blogspot.my/2010/12/walk-in-cloud.html

Gital, A. Y. u. & Zambuk, F. U. (2011). Cloud computing: Solution to ICT in higher education in Nigeria. Advances in Applied Science Research, 2(6), 364-369.

González-Martínez, J. A., Bote-Lorenzo, M. L., Gómez-Sánchez, E., & Cano-Parra, R. (2015). Cloud computing and education: A state-of-the-art survey. Computers & Education, 80, 132-151.

Gupta, N., & Thakur, S. (2014). The factors affecting the adoption of cloud computing technology in educational institutions. International Journal of Advanced Research in Computer and Communication Engineering, 3(6), 7229-7235.

Gupta, P., Seetharaman, A., & Raj, J. R. (2013). The usage and adoption of cloud computing by small and medium businesses. International Journal of Information Management,33(5), 861-874.

Goel S., et al .2011., "Impact of Cloud Computing on ERP implementations in Higher Education," International Journal of Advanced Computer Science and Applications, Volume 2/issue: 2(6), pp. 146-148, 2011.

Gruschka N and M. Jensen,2010 "Attack Surfaces: A Taxonomy for Attacks on Cloud Services," IEEE 3rd Intl. Conf. on Cloud Computing, 2010, pp. 276–279.

Gibbs, A. (2007). Focus Groups. Social Research Update, 19.

Green, B., Jones, M., Hughes, D., & Williams, A. (1999). Applying the Delphi Technique in a Study of GPs Information Requirements, Health & Social Care in the Community, 7(3), 198-205.

Gefen, D. & Ragowsky, A. (2005). A multi-level approach to measure the advantages of the associated ERP system in producing companies. Information Systems Management Journal, 22(1), 18 25.

Gamundani, A. M., Kanyangela, M., & Chitauro, S. (2015). A preliminary assessment of cloud computing e-learning solutions in South West Africa. Retrieved from https://www.researchgate.net/profile/Attlee_Gamundani/publication/281370580_A_Preliminary_Assessment_of_Cloud_Computing_Elearning_Solutions_in_Namibia/links/5606ca2808aeb5718ff76cc9.pdf

Hashemi, S. (2013). Cloud computing technology: Security and trust challenges. International Journal of Security, Privacy and Trust Management, 2(5), 1-7.

Hung, P. P., Bui, T.-A., Morales, M. A. G., Van Nguyen, M., & Huh, E.-N. (2014). The optimal collaboration of thin-thick clients and resource allocation in cloud computing. Personal and Ubiquitous Computing, 18(3), 563-572.

Hennink, M., Hutter, I., and Bailey, A. (2011). Qualitative Research Method. London: SAGE Publications Ltd.

Holstein, J. A., & Gubrium, J. F. (2003). Inside Interviewing: New Lenses, New Concerns: Thousand Oaks: Sage Publications.

Hauben, M., & Hauben, R. (1998). Behind the net: The untold story of the ARPANET and computer science. First Monday, 3.

Henneberger, M., & Luhn, A. (2010). Community clouds – supporting business ecosystems with cloud computing. Retrieved from http://www.sourcingfocus.com/uploaded/documents/Siemens_Community_Clouds_Whitepaper.pdf

Hashim, Hassan, & Hashim (2015). Climate studies, can students' perceptions of an ideal education environment be of use for institutional planning and resource utilization? Med Teach, 27 (4) (2005), pp. 332-337.

Hashemi, S. M., & Bardsiri, A. K. (2012). Cloud vs. grid computing. ARPN Journal of Systems and Software, 2(5), 188-194.

Hevner, A. R., Ram, S., March, S. T., & Park, J. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105.

Ibrahim, M. S., Salleh, N., & Misra, S. (2015). Empirical studies of cloud computing in education: A systematic literature review. Paper presented at the 15th International Conference on Computational Science and Its Applications, Alberta, Canada.

Ibrahim, M. S., Salleh, N., & Misra, S. (2015). Empirical studies of cloud computing in education: A systematic literature review. Paper presented at the 15th International Conference on Computational Science and Its Applications, Alberta, Canada.

IBM Global Technology Services. (2012). Applying the cloud in education: AN innovative approach. Retrieved from http://www-935.ibm.com/services/be/en/cloud-computing/cloud_edu_en.pdf

Irshad, M. B. M., & Johar, M. G. M. (2015). A study of the undergraduate use of cloud computing applications: Special reference to Google Docs. European Journal of Computer Science and Information Technology, 3(4), 22-32.

Islam, M. M., Morshed, S., & Goswami, P. (2013). Cloud computing: A survey on its limitations and potential solutions. International Journal of Computer Science Issues,10(4), 159-163.

Judy, E. (1995). The role of ARPA in the development of the ARPANET, 1961-1972. IEEE Annals of the History of Computing, 17(4), 76-81.

Jayasena K. P. N and H. Song, "Private Cloud with e-Learning for Resources Sharing in University Environment," in E-Learning, E-Education, and Online Training, Springer, Cham, 2017, pp. 169–180.

Khmelevsky, Y., & Voytenko, V. (2010). Cloud computing infrastructure prototype for university education and research. Paper presented at the 15th Western Canadian Conference on Computing Education, Kelowna, British Columbia, Canada.

King, N., and Horrocks, C. (2010). Interviews in Qualitative Research. London: SAGE Publications Ltd.

Koch, C. (2003). The ABC of ERP. Enterprise Resource Planning Research Centre. CIO. Kuhn, T. S. (1970). The Structure of Scientific Revolutions (2nd edition ed.). Chicago: University of Chicago Press.

Kanjo, C., 2008. Going beyond Diagnostics and Planning in ICT initiatives: Limitations in the context of Malawi, Prato CIRN 2008 Community Informatics Conference: ICTs for Social Inclusion: What is the Reality? 27- 30 October 2008, Plato, Italy, pp.1-17.

Kattimani, M.S.L., and Mallinath, M.W.K., 2017. Academic Resources Architecture Framework Planning using ERP in Cloud Computing. International Journal of Science and Research (IJSR) 6(2)

Kaur, K., & Rai, A. K. (2014). A comparative analysis: Grid, cluster, and cloud computing. International Journal of Advanced analysis in pc and Communication Engineering, 3(3), 5730-5734.

Khan M. A, "A Hybrid Cloud Computing Model for Higher Education Institutions in Saudi Arabia," in Cloud Computing, 2015, pp. 255–259.

Leedy, P. D. (1997). Practical Research – Planning and Design. pp. 104, Sixth Edition, Prentice-Hall, Inc. New Jersey.

Liamputtong, P. (2000). Qualitative Research Methods (3rd ed.): Oxford.

Liamputtong, P. (2009b). Qualitative Research Methods (3rd ed.): Oxford.

Linstone H. A. and Turoff M. (1975). The Delphi Method techniques and Applications. Addison-Wesley Pub Co., Reading, Massachusetts, pp. 535-549

Lehner, W., & Sattler, K.-U. (2010). Database as a service (DBaaS). Paper presented at the 26th IEEE International Conference on Data Engineering, Long Beach, California, USA.

Luke Ahmed. (2017). The Bell-LaPadula Model | Study Notes and Theory - A CISSP Study Guide. Retrieved June 8, 2019, from https://www.studynotesandtheory.com/single-post/The-Bell-LaPadula-Model

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. NIST Retrieved from http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505.

Murphy C., "ERP: The Once and Future King of Campus Computing," in Campus Technology, Syllabus Media Group, 2016. http://campustechnology.com/articles/2016/01/erp-the-once-and-future-king-of-campus-computing.aspx Accessed: 20th February 2018

Mokhtar, S. A., Ali, S. H. S., Al-Sharafi, A., & Aborujilah, A. (2013). Cloud computing in academic institutions. Paper presented at the 7th International Conference on Ubiquitous Information Management and Communication, Kota Kinabalu, Malaysia.

Moscato, F., Aversa, R., Di Martino, B., Fortis, T., & Munteanu, V. (2011). An analysis of mOSAIC ontology for cloud resources annotation. Paper presented at the 2011Federated Conference on Computer Science and Information Systems, Szczecin, Poland.

Madhav N. and M. K. Joseph, "Cloud-based Virtual Computing Labs for HEIs," in 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech), 2016, pp. 373–377.

Militaru G, A. A. Purcărea, O. D. Negoiţă, and A. Niculescu, “Examining Cloud Computing Adoption Intention in Higher Education: Exploratory Study,” in Exploring Services Science, 2016, pp. 732–741.

Musungwini S, B. Mugoniwa, S. S. Furusa, and T. G. Rebanowako, “An analysis of the use of cloud computing among university lecturers: a case study in Zimbabwe,” Int. J. Educ. Dev. Using Inf. Communication Technol. Bridget., vol. 12, no. 1, pp. 53–70, 2016.

Markey, S. C. (2013). Extend your secure development method to the cloud and extensive knowledge. Retrieved from https://www.ibm.com/developerworks/cloud/library/cl-extenddevtocloudbigdata/cl-extenddevtocloudbigdata-pdf.pdf

Mell, E, Grance, T. (2011). The NIST definition of cloud computing. November 22, 2018, from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Milić, A., Simić, K., & Milutinović, M. (2014). Cloud computing setting for E-Learning services for college students with disabilities. In Z. Mahmood (Ed.), Continued Rise of the Cloud (pp. 363-381). London: Springer.

Mohamed, A. (2009). History of cloud computing. Retrieved May 20, 2018, from http://www.computerweekly.com/feature/A-history-of-cloud-computing

Morsy A. M., Grundy J., Muller I. (2010). An Analysis of the Cloud Computing Security Problem. Retrieved October 25, 2018, from http://www.ict.swin.edu.au/personal/malmorsy/Pubs/cloud2010_1.pdf

Mowery, D. C., & Simcoe, T. (2002). Is the internet a US invention? An economic and technological history of computer networking. Research Policy, 31(8), 1369-1387.

Malhotra, N. K. (1999). Marketing Research: An Applied Orientation (International Edition ed.): Prentice Hall, Inc.

Malhotra, R., and Temponi, C. (2010). Critical decisions for ERP integration: Small business issues. International Journal of Information Management, 30(1), 28-37

Manaster, G. J., and Havighurst, R. J. (1972). Cross-National Research; Social-Psychological Methods and Problems, Boston: Houghton Mifflin

Maxwell, J. A. (2002). Understanding and Validity in Qualitative Research, In A.M. Huberman & M. B. Miles (Eds.), The Qualitative Researcher's Companion. SAGE Publications Ltd: London.

Maxwell, J. A. (2005). Qualitative Research Design: An interactive approach (2nd ed.). SAGE Publications Ltd: Thousand Oaks, California.

McNabb, D. E. (2012). Research methods in public administration and non-profit management: Quantitative and qualitative approaches. ME Sharpe.

Miles, M. B., and Huberman, A. M. (1994). Qualitative Data Analysis (2nd Edition ed.): SAGA Publications Ltd.

Myers, M. D. (2013). Qualitative research in business and management. SAGA Publications Ltd.

Myers, M. D., and Avison, D. (2002). Qualitative Research in Information Systems: SAGE Publications Ltd.

Mary Shacklett. (2016). Weighing the pros and cons of public versus hybrid clouds | ZDNet. Retrieved June 8, 2019, from https://www.zdnet.com/article/weighing-the-pros-and-cons-of-public-versus-hybrid-clouds/

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing— The business perspective. Decision Support Systems, 51(1), 176-189.

Mutiara, A., Refianti, R., & Witono, B. (2014). Developing a SAAS-cloud integrated development environment (IDE) for C, C++, and Java. Journal of Theoretical and Applied Information Technology, 68(1), 156-174.

Muli E, Kimuai J (2015) Adoption of cloud computing for education in Kenyan universities: challenges and opportunities. International Journal Advanced Research Computer Engineering Technology (IJARCET) 4(6)

Neto, M. D. (2014). A brief history of cloud computing. Retrieved April 20, 2018, from http://www.thoughtsoncloud.com/2014/03/a-brief-history-of-cloud-computing/

Neuman, W. L. (2005). Social Research Methods: Quantitative & Qualitative Approaches (7th edition ed.), Allyn, and Bacon.

Neuman, W. L. (2006). Social research methods: qualitative and quantitative approaches (6th ed.). Boston: Pearson/Allyn and Bacon.

Njeh, F. (2014). Cloud Computing: associate analysis of the Cloud Computing Adoption and Use Model. Bowie State University. Master thesis.

NIST (2009). The NIST Cloud Definition Framework. Retrieved March 14th, 2018 from http://csrc.nist.gov/groups/SNS/cloud-computing/cloud- computing-v26.pp

Okai, S., Uddin, M., Arshad, A., Alsaqour, R., & Shah, A. (2014). Cloud computing adoption model for universities to increase ICT proficiency. SAGE Open, 4(3), 215-234.

Ojala, A. (2013). Software-as-a-service revenue models. IT Professional, 15(3), 54-59.

Padron K.: Guide to Science Information Resources: Backward and Forward Reference Searching," Sept. 2017. Available on: http://libguides.fau.edu/c.php?g=325509&p=2182112

Pramod, N., Muppalla, A. K., & Srinivasa, K. (2013). Limitations and challenges in cloud-based application development. In Z. Mahmood & S. Saeed (Eds.), Software Engineering Frameworks for the Cloud Computing Paradigm (pp. 55-75). London: Springer.

Prasad, M. R., Naik, R. L., & Bapuji, V. (2013). Cloud computing: Research issues and implications. International Journal of Cloud Computing and Services Science, 2(2),134-140.

Pearson S., 2009 "Taking account of privacy when designing cloud computing services," ICSE W. on Software Engineering Challenges of Cloud Computing, 2009, pp. 44–52.

Pallis, G. (2010). Cloud computing: The new frontier of internet computing. IEEE Internet Computing, 14(5), 70-73.

Park, S.C., and Ryoo, S.Y. 2013. "An Empirical Investigation of End-users' switch Toward Cloud Computing: A 2 issue Theory Perspective," Computers in Human Behavior (29:1), pp.160-170

Pardeshi V. H, 2014 “Cloud Computing for Higher Education Institutes: Architecture, Strategy, and Recommendations for Effective Adaptation,” Procedia Econ. Finance, vol. 11, pp. 589–599, 2014.

Ramey J. and Rao P.G. 2011, “The systematic literature reviews as a research genre,” IEEE Intl. Professional Comm. Conf., 2011, pp. 1–7.

Rani, D., & Ranjan, R. K. (2014). A comparative study of SaaS, PaaS, and IaaS in cloud computing. International Journal of Advanced Research in Computer Science and Software Engineering, 4(6), 458-461.

Razak, S. F. A. (2009). Cloud computing in Malaysia universities. Paper presented at the2009 Conference on Innovative Technologies in Intelligent Systems and industrial applications, Kuala Lumpur, Malaysia.

Rajan, S., & Jairath, A. (2011). Cloud computing: The fifth generation of computing. Paper presented at the 2011 International Conference on Communication Systems and Network Technologies, Katra, Jammu, India.

Rao, K. S., & Challa, R. K. (2013). Adoption of cloud computing in education and learning. International Journal of Advanced Research in Computer and Communication Engineering, 2(10), 4160-4163.

Rocha F., S. Abreu, and M. Correia, “The Final Frontier: Confidentiality and Privacy in the Cloud,” IEEE Computer, vol. 44 (9), Sept. 2011, pp. 44–50.

Rao, S. S. (2000). Enterprise resource planning: business needs and technologies. Industrial Management & Data Systems, 100(2), 81–88.

Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1), 69-73.

Rose, J., & Fogarty, G. J. (2006). Determinants of perceived usefulness and perceived ease of use in the technology acceptance model: Senior consumers' adoption of self-service banking technologies. Paper presented at the Conference of the Academy of World Business, Marketing and Management Development, Paris, France.

Rahimah K. and N. Aziati, “The Integrated Framework of Cloud Computing Implementation in Higher Education Institution: A Review of Literature,” Adv. Sci. Lett., vol. 23, no. 2, pp. 1475–1479, Feb. 2017.

Sachdeva, M., Rana, P., Kapoor, R., & Shahid, M. (2011). Cloud computing-pay as you go technology. Paper presented at the 5th National Conference on Computing for National Development, New Delhi, India.

Sabahi, F. (2011a). Cloud computing reliability, availability, and serviceability (RAS): Issues and challenges. International Journal on Advances in ICT for Emerging Regions, 4(2),12-23.

Sabahi, F. (2011b). Cloud computing security threats and responses. Paper presented at the IEEE 3rd International Conference on Communication Software and Networks, Xi'an, China.

Sabi, H. M., Uzoka, F.-M. E., Langmia, K., & Njeh, F. N. (2016). Conceptualizing a model for adoption of cloud computing in education. International Journal of Information Management, 36(2), 183-191.

Sajid, M., & Raza, Z. (2013). Cloud computing: Issues & challenges. Paper presented at the International Conference on Cloud, Big Data, and Trust, Bhopal, Madhya Pradesh, India.

Shawish, A., & Salama, M. (2014). Cloud computing: paradigms and technologies. In F. Xhafa & N. Bessis (Eds.), Inter-cooperative Collective Intelligence: Techniques and applications (pp. 39-67). Berlin Heidelberg: Springer.

Sheng, X., Tang, J., Xiao, X., & Xue, G. (2013). Sensing as a service: Challenges, solutions, and future directions. IEEE Sensors Journal, 13(10), 3733-3741.

Singh, A., & Hemalatha, M. (2012). Cloud computing for an academic environment. International Journal of Information and Communication Technology Research, 2(2),97-101.

Sommer, Y. (2014). Azure vs. Amazon web services: A keen & dynamic comparison for small business owners. Retrieved March 20, 2018, from http://cswsolutions.com/blog/azure- vs-amazon-web-services-keen-dynamic-comparison-small-business-owners/

Singh S. Y.-S. Jeong, and J. H. Park, 2016 “A survey on cloud computing security: Issues, threats, and solutions,” J. Network. Computer. Appl., vol. 75, Nov. 2016, pp. 200–222.

Shinder T.W, Y. Diogenes, and D.L. Shinder, "Windows Server 2012 security from end to edge and beyond: architecting, designing, planning, and deploying Windows Server 2012 security solution," Elsevier, 2013.

Segrelles J.D and G. Moltó, “Assessment of cloud-based Computational Environments for higher education,” in 2016 IEEE Frontiers in Education Conference (FIE), 2016, pp. 1–9.

Shadreck Chitauro, 2017 “Designing A Cloud-Based E-learning Implementation Model for Higher and Tertiary Institutions in Namibia” Namibia University of Science and Technology. Master Thesis

Sen, J. (2013). Security and privacy issues in cloud computing. In A. R. Martínez, F. P. García, & R. Marín-López (Eds.), Architectures and Protocols for Secure Information Technology Infrastructures (pp. 1-45): IGI Global.

Shinder T.W. (2011, August 3). Security Issues in Cloud Deployment model. TechNet Articles, p. 2. Retrieved on August 3rd., 2018 from http://social.technet.microsoft.com/wiki/contents/articles/security-issues-in-cloud-deployment-models.aspx from TechNet database.

Skiba, D. J. (2011). Are you computing in the clouds? Understanding cloud computing. Nursing Education Perspectives, 32(4), 266-268.

Subra, K. (2011). Introduction to Cloud Security design from a Cloud Consumer's Perspective. Anna University Tirunelveli, Tirunelveli

Sukumaran, K. (2011). The perspective of cloud computing applications in professional education. Journal of Modern Education Review, 1(2), 89-98.

Schofield, J. W. (2002). Increasing the Generalizability of Qualitative Research. In A. M. Huberman & M. B. Miles (Eds.), The Qualitative Researcher's Companion. London: SAGE Publications Ltd.

Silverman, D. (2013). Doing qualitative research: A practical handbook. SAGE Publications Ltd.

Stake, R. (1995). The art of case study research. Thousand Oaks, CA: Sage Publications Ltd.

Sheng Y, L. Zhu, S. Changxiang, Multilevel security Model, Computer Engineering and Design, 31 (13), 2010.

Sandhu R, Lattice-based Access Control Models, IEEE Computer, 26(11), pp. 9-19, 1993.

Surjeet Kumar Yadav and Saurabh pal (2012). Data Mining Application Enrollment Management: A Case Study. International Journal of Computer Applications. International Journal of Computer Applications 41 (5), March 2012 (0975 –8887)

Tan, X., & Kim, Y. (2011). Cloud computing for education: A case of using Google Docs in MBA group projects. Paper presented at the2011 International Conference on Business Computing and Global Information, Shanghai, China.

Tashkandi, A., & Al-Jabri, I. M. (2015). Cloud computing adoption by higher education institutions in Saudi Arabia. Paper presented at the 2015 International Conference on Cloud Computing, Riyadh, Saudi Arabia.

Tian, W., & Zhao, Y. (2015). An introduction to cloud computing Optimized Cloud Resource Management and Scheduling (pp. 1-15). Boston: Morgan Kaufmann.

Truong, H.-L., Pham, T.-V., Thoai, N., & Dustdar, S. (2012). Cloud computing for education and research in developing countries. In L. Chao (Ed.), Cloud Computing for Teaching and Learning: Strategies for Design and Implementation (pp. 64-80): IGI Global.

The CIA Principle." [Online]. Available: http://www.doc.ic.ac.uk/~ajs300/security/CIA.htm. [Accessed: 15 Mar. 2018].

Trovati M, S.Y. Zhu, and R. Hill, 2015 "Guide to security assurance for cloud computing," Springer, 2015.

Tashkandi A. N and I. M. Al-Jabri, "Cloud computing adoption by higher education institutions in Saudi Arabia: an exploratory study," Cluster Computer, vol. 18, no. 4, pp. 1527–1537, Dec. 2015.

Tsai, W. H., Lee, P. L., Shen, Y. S., and Lin, H. L. (2012). A comprehensive study of the relationship between enterprise resource planning selection criteria and enterprise resource planning system success. Information & Management, 49(1), 36-46.

Tejal, V. D., & Mathur, S. K. (2014). Adoption of cloud computing by tertiary level students: A study. Journal of Exclusive Management Science, 3(3), 1-15.

Tsai, W.-T., Sun, X., & Balasooriya, J. (2010). Service-oriented cloud computing architecture. Paper presented at the 2010 Seventh International Conference on Information Technology: New Generations, Las Vegas, Nevada, USA.

U. Hoyer and H. Obel, "Guide on SaaS vs. PaaS and IaaS. Available: https://www.linkedin.com/pulse/guide-saas-vs-paas-iaas-ulrik-hoyer-hansen-obel[Accessed: 29 June 2018].

Verma, A., & Kaushal, S. (2011). Cloud computing security issues and challenges: A survey. Paper presented at the International Conference on advances in computing and communications, Kochi, India.

Verma, R. P., Dutta, S., Chaulya, S., Singh, A., & Prasad, G. (2013). Cloud computing: A new era in the IT industry. International Journal of Computer Technology and Electronics Engineering, 3(2), 18-28.

Velte, A. T., Velte, T. J., & Elsenpeter, R. (2010). Cloud computing: A practical approach. New York: McGraw-Hill, Inc.

Vecchiola, C., Chu, X., & Buyya, R. (2009). Aneka: A software platform for .NET-based cloud computing. High Speed and Large-Scale Scientific Computing, 18, 267-295.

Vandaie, R. (2008). The role of organizational knowledge management in successful ERP implementation projects. Knowledge-Based Systems, 21, 920–926.

Venkatachalam Ragupathy and Arts Chen Shu-Heng, (2017). Agent-based modeling as a foundation for big data. Journal of Economic Methodology 24 (4):362-383

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2009). A break in the clouds: Towards a cloud definition. ACM SIGCOMM Computer Communication Review, 39(1), 50-55.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2011). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478.

Voas, J., & Zhang, J. (2009). Cloud computing: New wine or just a new bottle? IT Professional, 11(2), 15-17.

Wang, L., Tao, J., Kunze, M., Castellanos, A. C., Kramer, D., & Karl, W. (2008). Scientific cloud computing: Early definition and experience. Paper presented at the 10th IEEE International Conference on High-Performance Computing and Communications, Dalian, China.

Wiedemann, D., & Strebel, J. (2011). Organizational determinants of corporate IaaS usage. Paper presented at the 2011 IEEE 13th Conference on Commerce and Enterprise Computing, Luxembourg-Kirchberg, Luxembourg.

Writer, S. (2015). Cloud through the ages: 1950s to the present day. Retrieved March 20, 2018, from http://www.thoughtsoncloud.com/2015/04/a-brief-history-of-cloud-1950-topresent-day/

Wei L. et al., "Security and privacy for storage and computation in cloud computing," Inf. Sci. (NY)., vol. 258, pp. 371–386, Feb. 2014.

Watson, T. (2008). Public Relations Research Priorities: A Delphi Study. Journal of Communication Management. 12(2), 104-123.

Weideman, A. (2013). Positivism and Post-positivism. The Encyclopedia of Applied Linguistics.

Williamson, K. (2002a). Research Methods for Students, Academics, and Professionals: Information Management and Systems (2nd ed.): Charles Stuart University, NSW.

Williamson, K. (2002c). Research Techniques: Questionnaires and Interviews Research Methods for Students, Academics, and Professionals (pp. 235-249). Charles Stuart University, NSW.

Williamson, K., Burstein, F., and McKemmish, S. (2002). The Two Major Traditions of Research. In P. R. Harvey & D. S. Ferguson (Eds.), Research Methods for Students, Academics, and Professionals: Information Management and Systems (2nd ed.): Charles Stuart University, NSW.

Wikipedia. (n.d.). Biba Model Wikipedia. Retrieved June 8, 2019, from

Williams, B., Brown, T., & Onsman, A. (2012). Exploratory factor analysis: A five-step guide for novices. Australasian Journal of Paramedicine, 8(3), 1-13.

Yin, R. K. (2014). Case study research: design and methods (5th ed.). Los Angeles: SAGE.

Yin, R. (2003). Case Study Research: Design and methods (3rd ed.). Thousand Oaks, CA: Sage Publications Ltd. https://en.wikipedia.org/wiki/Biba_Model

Yanming, L, D. Qingkuan, Li. Xiaoping, Study on Enhancing Integrity for BLP Model, Journal on communications, 31(2), 2010.

Yin, R. K. (2014). Case Study Research: Design And Methods (5th ed.). Los Angeles: SAGE.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7-18.

APPENDICES

Appendix A: Transmitter letter

KAMPALA INTERNATIONAL UNIVERSITY
EXPLORING THE HEIGHTS

Ggaba Road, Kansanga * PO BOX 20000 Kampala, Uganda
Tel: 0772365060 Fax: +256 (0) 41 - 501974 E-mail:
dhdrinquiries@kiu.ac.ug * Website: http://www.kiu.ac.ug

Directorate of Higher Degrees and Research
Office of the Director

Our ref. 1165-04256-10227

Monday 4th June, 2018

Dear Sir/Madam,

RE: INTRODUCTION LETTER FOR IBRAHIM ADABARA

REG. NO. 1165-04256-10227

The above mentioned candidate is a student of Kampala International University pursuing a Master of Science in Information Technology.

He is interested in conducting a research for his dissertation titled, ***"A Model for Cloud-Based Academic Enterprise Resource Planning (CAERP) for a higher institution".***

Your organization has been identified as a valuable source of information pertaining to the research subject of interest. The purpose of this letter is to request you to kindly cooperate and avail the researcher with the pertinent information he may need. It is our belief that the findings from this research will benefit KIU and your organization.

Any information shared with the researcher will be used for academic purposes only and shall be kept with utmost confidentiality.

I appreciate any assistance rendered to the researcher

Yours Sincerely,

Dr. Claire M. Mugasa
Director

04 JUN 2018
for DIRECTOR DHDA
Dep. Dir.

C.c. DVC, Academic Affairs
Dean, SCIT

"Exploring the Heights"

Appendix B: Consent letter

A MODEL FOR CLOUD-BASED ACADEMIC ENTERPRISE RESOURCE PLANNING (CAERP) FOR A HIGHER INSTITUTION

Dear Respondent,

I am conducting a study on 'A Model for Cloud-Based Academic Enterprise Resource Planning (CAERP) for a higher institution' at Kampala International University, Uganda. The objective of this research is to develop A Security Model for Cloud-Based Academic Enterprise Resource Planning (CAERP) For A Higher Institution. Your participation will help in developing the final security model for my study.

Your participation is voluntary, and the result of this study will be used for academic purposes only. Your participation is much appreciated since this research will add to the development of A Model for Cloud-Based Academic Enterprise Resource Planning (CAERP) For A Higher Institution and will be useful in the design and development of ERP systems in the future.

If you have any questions or concerns about completing the questions or about participating in this study, you may contact me on +256772019794, +256754012291, or email at adabara360@gmail.com. If you have any questions about your rights as a research subject, you may contact my Supervisors.

Dr. Sanni Shamsudeen (sanniade01@gmail.com). Find attached is the transmitter letter

Sincerely,

Ibrahim Adabara

Appendix C: ICT Director interview questions

1. Do you have any ERP platform?
2. How often do you upgrade your ERP system?
3. What ERP technologies do you use?
4. How do you use the ERP system to enhance the institution's service?
5. Does the ERP system help to generate daily, monthly, and or yearly reports?
6. What challenges are information security facing in the using an ERP system?
7. What challenges are identity security facing in the using an ERP system?
8. Understand the networking department of Uganda communications currently running a project of implementing a private cloud locally. How far have they gone with the plan?
9. How do you think the On-Premises system could be improved?
10. Do you have any plans to migrate or transfer the current server base ERP platform to the cloud?
11. Just for clarity, I was considering moving the server-based ERP as a service on the cloud, and you and other systems administrators keep on administering it. Do you think there will be problems or issues regarding hardware and physical infrastructure?
12. If we go to the public cloud way, many stakeholders are skeptical about it. However, when you go cloud, you will sign Service-level agreement (SLA) confidentiality documents so that your information will be secured. What is your comment about that?
13. Thank you very much for your input. Are there any other comments on what you feel about the ERP server which we did not ask but that you think is essential, and we need to be aware of?

Appendix D: Hardware system analyst interview questions

1. Do you have any ERP platform?
2. On another note, what are the tools (e.g., computers) or infrastructure required by the users to access the ERP platform?
3. What are the current specifications on the institution`s ERP server?
4. Can you discuss key technical challenges you are facing concerning the use or management of the institution ERP system?
5. On the issue of backup, you are responsible for backing up the whole system or individual data. For the sake of space, do you have a separate backup server, or it is up to the administrators of the system?
6. What is the architecture for the cloud in the higher institution, including various service and deployment models?
7. What challenges are infrastructure security facing in the using an ERP system?
8. What type of hardware security problems do you experience with the ERP system?
9. What type of network security problems do you experience with the ERP system?
10. How does the backup work, how do you back up the system?
11. What is the strategy for the active implementation cloud environment in higher institutions?
12. I understand the current system is a single sign-on, maybe just a comment on integrating two-way authentication on the current project.
13. I understand you are running server-based ERP. Can you describe the setup of the server-based ERP regarding infrastructure?
14. I understand you are using server-based ERP; can you describe its setup regarding infrastructure and technical requirements as well as users' feedback, and the tools required by users to access the platform?
15. What are the significant challenges (technical) faced with the current platform?
16. What type of security problems do you experience with the ERP system?
17. Do you need to change/acquire (sufficient infrastructure) (if any) to migrate the current ERP system to the cloud?

Appendix E: Software systems analyst interview questions

1. Do you have any ERP platform?
2. What ERP technologies do you use?
3. How long does it take to generate consolidated reports using an ERP system?
4. What are the current specifications on the institution`s ERP server?
5. What are some of the technical challenges?
6. Who are the people responsible for the creation of user accounts on the institution's ERP server?
7. All users' accounts at this institution are created on the server-based ERP and any comment about the most recent security challenges in particular on this issue?
8. What challenges are software security facing in the using an ERP system?
9. What type of data security problems do you experience with the ERP system?
10. I understand the institution's ERP system supports remote access from campus, and users can connect from those remote sites to the ERP platform. Have you encountered or receive comments concerning challenges been faced by remote user's access with regards to speed and bandwidth?
11. Just for clarity, I was considering moving the server-based ERP as a service on the cloud, and you and other systems administrators keep on administering it. You will not be worried about hardware and physical infrastructure. Do you think there will be problems or issues regarding hardware and physical infrastructure?
12. Do you think the infrastructure the higher institution already had can access the cloud server or the higher institution need to supply or add more equipment, bandwidth, and other aspects?
13. Thank you very much for your input. Are there any other comments on what you feel about the ERP server which we did not ask but that you think is essential, and we need to be aware of that?