UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

RESEARCH PROJECT REPORT

A DATA SECURITY IMPLEMENTATION MODEL FOR CLOUD COMPUTING IN GOVERNMENT PARASTATALS

MUTHEE JOSEPHINE W.

SUPERVISOR: DR. ELISHA ABADE

P54/65180/2013

A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF COMPUTING AND INFORMATICS IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF A DEGREE IN MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT OF THE UNIVERSITY OF NAIROBI.

August 2016

DECLARATION

This research project is my own original work and has not been presented for the award of degree in other university

Signature: …… Date: ……..……..……

MUTHEE JOSEPHINE WANJIRA

REG NO: P54/65180/2013

This research project has been submitted for examination with my approval as university supervisor

Signature: _____ Date_____

DR. ELISHA ABADE

School of Computing and Informatics

University of Nairobi.

DEDICATION

This project is dedicated to my loving mum Beatrice Muthee.

ACKNOWLEDGEMENTS

My heartfelt sincere gratitude is to the Almighty God for his grace and providing me good health, sound mind and the knowledge to complete this project to its conclusion.

Most important, I sincerely wish to acknowledge the support from my supervisor Dr. Elisha Abade for his wisdom, support and without whom I could not have gone this far with my project work.

I specially thank my darling husband Bernard for his moral, financial support and understanding, our children Victor and Amelia for their understanding and love.

To all my lecturers who contributed in one way or another in quenching my desire for knowledge I owe you my gratitude. I owe a great deal of gratitude to my family members for their unfailing encouragement and moral support throughout my period of study and for understanding and appreciating the demand of the course in terms of time and resources.

ABSTRACT

Cloud computing has transformed the way organisations approach technology enabling them to introduce new business models, provide more services and reduce IT costs. This research project aims at investigating the types of cloud implemented, analyse challenges and techniques used to overcome and finally design a data security implementation model for cloud computing in government parastatals. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models and can coexist with other technologies and software design approaches. Cloud computing presents a huge dilemma for security professionals. Maintaining control over cloud data is paramount to cloud success. It is a strike between risks involved and the economic benefits. There are many concerns that arise while seeking to implement cloud technologies. They include security and privacy, identification and authentication, authorisation, confidentiality, integrity, non repudiation and availability among others. This research identified six government parastatals that are IT- enabled and have hosted some of their applications on cloud. The target group of respondents for this research are managers and employees in the Information Technology departments in randomly selected governmental parastatals.

The proposed model borrows most of its content from other developed frameworks and from the results of the survey. This assists in the mapping out of data security areas and controls that will be of use to prospective cloud users. A thorough quantitative analysis will be undertaken to ensure credibility. Excel tool will be used to analyse data. The research design is descriptive. The data collection technique is a purposive survey research using sampling and questionnaires. Our sample size is 42 respondents. Questionnaires were used with 22 respondents giving valid feedback. They agreed that it is paramount to ensure data security during implementation of cloud solutions, the model covers the following areas discovery of cloud services and deployment models, CSP , defining governance, risk compliance and access management procedures, drawing SLA, QoS, ownership contracts, data life cycle security procedures, developing capacity plans, resource management, provisioning, cloud management and monitoring plans, testing different cloud layers data security metrics and finally implementing the cloud solution.

The implication of this research is that government parastatals can now regain their trust in this paradigm and consider implementing more system in the cloud and those that have vast ICT resource to offer those that do not inform of cloud solution where as CSP thereby maximizing on the benefits that cloud computing offers and reducing government expenditure on new infrastructure, hardware, software and manpower. Since data security is one of the major hindrance in the implementation of cloud computing, this research proposes a six step model that could be employed by government parastatals to ensure data security in their cloud.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AAA	-	Authentication, authorization, and accounting
BPO	-	Business Process Outsourcing
COA	-	Collaboration Oriented Architecture
CPU	-	Central Processing Unit
CSA	-	Cloud Security Alliance
DLP	-	data leakage prevention
DMZ	-	Demilitarized Zone
ENISA	-	European Network and Information Security Agency
GDC	-	Government Data Center
GRC	-	Governance, Risk Management, and Compliance
IaaS	-	Infrastructure as a Service
ICTA	-	Information Communication Technology Authority
IETF	-	Internet Engineering Task Force
ISACA	-	Information Systems Audit and Control Association
ISP	-	Internet Service Provider
ITES	-	Information Technology enabled services
ITU	-	International Telecommunication Union
KPTC	-	Kenya Posts and Telecommunications Corporation
MTP	-	Medium Term Plans
NIST	-	National Institute of Standards and Technology
OCCI	-	Open Cloud Computing Interface
OVF	-	Open Virtualization Format
PaaS	-	Platform as a Service
QoS	-	Quality of Service
RSA	-	Ron Rivest, Adi Shamir and Leonard Adleman
SaaS	-	Software as a Service
SAP	-	SSL Authentication Protocol
SHA	-	Secure Hash Algorithm

SME - Small and Medium-sized Enterprises

SPSS - Statistical Package for the Social Sciences

SSL - Secure Sockets Layer

SWOT - Strengths, Weaknesses, Opportunities, and Threats

TCG - Trusted Computing Group

TCP - Trusted Computing Platform

UA - User Authentication

VPN - Virtual Private Network

ACLs - Access Control Lists

CDSM - Cloud data security implementation Model

COBIT - Control Objectives for Information and related Technology

CRAM - Cloud Risk Accumulation Model

CSP - Cloud Service Provider

DOS - Denial of Service

DR - Data Recovery

GCCN - Government Common Core Network

GDP - Gross Domestic Product

I/O - - Input/Output

ICT - - Information & Communications Technology

IS - - Information System

ISO - - International Organization for Standardization

IT - - Information Technology

ITIL - - Information Technology Infrastructure Library

KENET - Kenya Education Network Trust

MD5 - - Message Digest algorithm

NDA - - Non disclosure agreements

NOFBI - - National Optic Fibre Backbone Infrastructure

OLA - Operation Level Agreement

PCI - Payment Card Industry

R&D - - Research and Development

SA - - Security Architecture

SACS - - Security Access Control Service

SDLC - - security Software or solution or system Development Life Cycle

SLA - - Service Level Agreement

SP - - Service Provider

SSF - - Store Small Files

SW - Software

TC - Trusted Computing

TCP - Trusted Computing Platform

VM - Virtual Machine

DEFINITION OF TERMS

Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services.

Access control list (**ACL**) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list.

Cloud: A set of hardware, networks, storage, services, and interfaces that enable the delivery of computing as a service.

Disaster recovery (DR) site is a facility an organization can use to recover and restore its technology infrastructure and operations when its primary data centre becomes unavailable.

IaaS: **Infrastructure as a Service** is a provision model based on the need for equipment outsourcing to support daily operations. This service model provides virtual machines, virtual storage, virtual infrastructure and other hardware assets as resources. In this model, service provider is responsible for managing all the infrastructure. On the other hand, some responsibilities exist for the clients which are operating system, applications and user interaction with the system.

PaaS: Platform as a Service is a provision model based on the need for computing platform and solution stack. Provision of virtual machines, operating systems, development frameworks describes the goal of PaaS. Service provider responsibilities are managing cloud infrastructure, the operating system and enabling software. Clients responsibilities can be listed as application deployment or application use supported by PaaS, installing and managing the application.

SaaS: Software as a Service is a software licensing and delivery model. This service model is a complete operating environment with applications, management and user interface. In SaaS, service provider is responsible for everything from the application down to the infrastructure. Clients are responsible for entering and managing its data and user interaction in this service model.

Public cloud: These type of clouds are owned by an organization. Point of interest is selling cloud services.

Private cloud: Clouds operated for the exclusive use of an organization. Either managed by that organization or a third party.

Hybrid cloud: These type of clouds are combination of both public and private.

Business continuity planning (BCP) - is a broad disaster recovery approach whereby enterprises plan for recovery of the entire business process. This includes a plan for workspaces, telephones, workstations, servers, applications, network connections and any other resources required in the business process (Gartner, 2013).

Cloud bursting - is the use of an alternative set of public or private cloud-based services as a way to augment and handle peaks in IT system requirements at startup or during runtime. Cloud bursting can span between on-premises IT systems and services and the cloud, across multiple cloud providers or across multiple resource pools of a single provider. It can also be enabled across multiple internal data centers, across multiple external data centers, or between internal and external data centers (Gartner, 2013).

Compliance - The process of adhering to policies and decisions. Policies can be derived from internal directives, procedures and requirements, or from external laws, regulations, standards and agreements (Gartner, 2013).

Cloud Computing - Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models (NIST, 2011)

Cyber Incident Response Plan (CIRP) - Also known as a "computer incident response plan," this is formulated by an enterprise to respond to potentially catastrophic, computer-related incidents, such as viruses or hacker attacks. The CIRP should include steps to determine whether the incident originated from a malicious source — and, if so, to contain the threat and isolate the enterprise from the attacker (Gartner, 2013).

Cyber Forensics - the use of specialized, investigative techniques and technologies to determine whether illegal or otherwise inappropriate events have occurred on the Web, and provide legally defensible information about the sequence of those events (Gartner, 2013).

Disaster recovery (DR) **-** is defined as (1) The use of alternative network circuits to re-establish communications channels in the event that the primary channels are disconnected or malfunctioning, and (2) The methods and procedures for returning a data center to full operation after a catastrophic interruption e.g., including recovery of lost data (Gartner, 2013).

Endpoint protection platform (EPP) - is a solution that converges endpoint device security functionality into a single product that delivers antivirus, anti-spyware, personal firewall, application control and other styles of host intrusion prevention (for example, behavioral blocking) capabilities into a single and cohesive solution. (Gartner, 2013)

Federated identity management - enables identity information to be developed and shared among several entities and across trust domains. Tools and standards permit identity attributes to be transferred from one trusted identifying and authenticating entity to another for authentication, authorization and other purposes, thus providing "single sign-on" convenience and efficiencies to identified individuals, identity providers and relying parties (Gartner, 2013).

Grid Computing - A method for applying large numbers of resources, usually large amounts of processing capacity, to a single task, by applying resources from more than one system. A grid is a collection of resources that's coordinated to enable the resources to solve a common problem. A computing grid harnesses multiple computers from several owners to run one very large application problem (Gartner, 2013).

Identity and access management (IAM) - is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons. IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements. This security practice is a crucial undertaking for any enterprise (Gartner, 2013).

Lightweight Directory Access Protocol (LDAP) - is an Internet protocol that email and other programs use to look up information from a server (Gartner, 2013).

Measured Service - Customers' use of the capabilities is monitored, controlled, reported, and charged; with complete transparency enabling a pay-as-you-consume metering arrangement (NIST, 2011).

Multi-tenancy - enables sharing of resources and costs across a large pool of users thus allowing for centralization of infrastructure, Peak-load capacity increases and utilization and efficiency improvements for systems that are often only 10–20% utilized. The instances (tenants) are logically isolated, but physically integrated. The degree of logical isolation must be complete, but the degree of physical integration will vary (Gartner, 2013).

On-demand self-service - Customers can unilaterally provision computing capabilities, without requiring human interaction with the service provider (NIST, 2011).

Portability - In cloud computing terminology, the phrase "cloud portability" means the ability to move applications and its associated data between one cloud provider and another -- or between public and private cloud environments (Gartner, 2013).

Rapid elasticity - Near-immediate provisioning of capabilities, to quickly scale up, or down, according to demand (NIST, 2011).

Resource pooling - Physical and virtual resources are dynamically assigned and reassigned according to demand, resulting in cost savings to the customer (NIST, 2011).

Sandbox - is a security mechanism for separating running programs. It is often used to execute untested code or untrusted programs from unverified third-parties, suppliers, untrusted users and untrusted websites. The sandbox typically provides a tightly controlled set of resources for guest programs to run in, such as scratch space on disk and memory. Network access, the ability to inspect the host system or read from input devices are usually disallowed or heavily restricted. In this sense, sandboxes are a specific example of virtualization (Gartner, 2013).

Service-Level Agreement (SLA) - An agreement that sets the expectations between the service provider and the customer and describes the products or services to be delivered, the single point of contact for end-user problems and the metrics by which the effectiveness of the process is monitored and approved (Gartner, 2013).

Secure Socket Layers (SSL) - is the standard **security** technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral

Unified threat management (UTM) - is a converged platform of point security products, particularly suited to small and midsize businesses (SMBs). Typical feature sets fall into three main subsets, all within the UTM: firewall/intrusion prevention system (IPS)/virtual private network, secure Web gateway security (URL filtering, Web antivirus [AV]) and messaging security - anti-spam, mail AV (Gartner, 2013).

User authentication technologies - encompass a variety of products and services implementing a range of authentication methods in place of legacy passwords. Authentication may be natively supported in products or services (including other security tools), or provided by discrete software, hardware or cloud-based services (Gartner, 2013).

A **virtual machine (VM)** - is a software implementation of a hardware-like architecture, which executes predefined instructions in a fashion similar to a physical Central processing unit (CPU). A VM can be used to create a cross-platform computing environment that loads and runs on computers independently of their underlying CPUs and operating systems. (Gartner, 2013)

CHAPTER 1

INTRODUCTION

1.1 Background information

Kenya is a third world developing country located in the East Coast of Africa. The core development principles and the objectives are set out in a vision 2030 statement which was published in 2006 and is to be implemented through a succession of five-year medium term plans (MTP). The Kenya ICT master plan outlines the three key Pillars in the Vision 2030 as Economic, Social, and Political. Vision 2030 through the economy pillar aspires to build an economy with highly ambitious growth rate of 10% p.a accompanied by improved governance and social welfare. ICT is one of the foundations for economic development in the second MTP of Vision 2030, with the theme, "strengthening the foundation for a knowledge economy". ICT is a critical tool in Kenya's vision of knowledge based economy, which aims at shifting the current industrial development path towards innovation where creation, adoption, adaptation and use of knowledge as the key source of economic growth are key.(ICT Authority, 2014) ICT and telecommunications has been a dynamic growth sector in the economy in recent years, and national development plans have sought to exploit its potential by promoting business process outsourcing (BPO) and IT-enabled services (ITES) (Souter and Makau, 2012).

1.1.1 Internet and ICT

Internet since its inception has been a major drive towards the various technologies developed today. In Kenya internet was first noted in 1990s but 1995 marks the start of the country's formal Internet development with the establishment of the first (unlicensed) commercial ISPs and formation of a study group to consider options for the 'Internet phenomenon' by the Kenya Posts and Telecommunications Corporation (KPTC, the government-owned Telco). By 2000, access to the Internet was available through a number of competing ISPs and some 250 cyber cafes, about half of which were located in Nairobi. (Souter and Makau, 2012) Until mid 2009, Kenya like the rest of the East African countries relied solely on satellite for internet connectivity and international communication. According the Kenya engineer an increasing number of Kenyan individuals, households and organizations are now connected to the Internet. The Internet penetration in Kenya was 64.3% representing 26.1 million users according to the Communication Authority (see http://www.ca.go.ke). Mobile Internet subscriptions were about 16.3 million which is over 99% of all subscriptions in Kenya. But there were 81.243 fixed fiber optic data subscriptions and 17,537 terrestrial wireless data subscriptions.

Subsequently, the country is connected to the international broadband highway through the SEACOM, TEAMS, EASSY, and LION undersea fibre cables. Most major towns in Kenya are connected through the National Optic Fibre Backbone Infrastructure (NOFBI).

The Government has also developed a Government Common Core Network (GCCN). This is meant to serve as a shared and secure interoperable Government-wide ICT architecture. The system will not only integrate work processes and information flows, but also improve inter-ministerial sharing of databases and exchange of information to eliminate duplication and redundancies, improve public access to Government services and ensure responsiveness in reporting, monitoring and evaluation (Kenya e-Government Master Plan, 2013).

In addition, the Government developed the tier-2 Government Data Centre (GDC) infrastructure to ensure security of Government data and applications. Bandwidth support to Government offices has been steadily growing. Furthermore, the Government through the national treasury is implementing a disaster recovery facility for data and systems as part of the business continuity plan. This will ensure that the Government services continue to be provided even in case of any disaster at the primary sites. This facility will also offer an environment for cloud computing to offer services by the County Governments. (ICT Authority, 2014)

Government has high aspirations for use of the Internet, notably in developing export-oriented IT-enabled service sectors and for improving the delivery of public services. These aspirations are based on assumptions about the relationship between Internet, broadband and socio-economic outcomes which are widely held within the international ICT community,

1.1.2 Cloud Computing

Surprisingly little attention seems to be paid at present to the potential for cloud computing, which has significant implications for the fulfilment of government objectives in BPO and IT-enabled services, though this was one of the themes for discussion during the 2011 Kenya Internet Governance Forum(IGF). (Souter and Makau, 2012)

Cloud computing is one of the recent internet technologies in the ICT evolution of the last few decades. Arguably, one of the many definitions of cloud computing defines it as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage devices and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Catteddu and Hogben, 2009). People are adapting to it where they can have everything they need on the cloud. The Cloud is a metaphor for the

Internet, based on how it is depicted in computer network diagrams, and is an abstraction for the complex infrastructure it conceals.

Many of the advances in ICT service delivery have been the result of networking innovations. Initially, the new breakthroughs were disruptive. But in each case, the uncertainty, doubts, and technological barriers were eventually overcome.

Cloud computing is therefore not an exception. Government, education, and healthcare organizations are embracing clouds as a way to increase their operational efficiency and productivity, while at the same time maximizing investments and lowering costs. (Macias and Greg, 2011)

Cloud computing is a low-cost viable option to users (Gens F, 2009). In addition, Building a high-availability cloud infrastructure does not have to be a laborious, costly proposition. Most ICT groups can use their existing infrastructure, which is likely to be underused at present. Transitioning to a cloud environment may be more about new thinking than it is about new technology. (Macias and Greg, 2011)

Due to the nature and demand of emerging cloud technologies, there is a certain degree of inexperience when dealing with cloud security. Currently Cloud computing clients have to trust 3rd party cloud providers on many fronts, especially on the availability of cloud service as well as data security. Therefore the SLA forms an integral part of a client's first line of defence.

In providing a secure Cloud computing solution, a major decision is to decide on the type of cloud to be implemented. Currently there are three types of cloud deployment models offered, namely, a public, private and hybrid cloud.

The utilization of the private cloud is more pronounced than public. There are more organizations utilizing pure private cloud (39%) than those utilizing a public cloud (22%). The remaining organizations are utilizing both private and public or are yet to adopt.

Though all systems have been implemented in Kenya, the Iasi option is the most prominent. The government therefore should champion cloud services by adopting use of the cloud to provide services and thus it would set pace for better uptake by the private sector. It should also enhance relevant legal and regulatory frameworks for protection of cloud service users, addressing cyber security challenges, guaranteeing secure online payments, privacy and data security. (Omwansa, Waema and Omwenga, 2014)

This project research aim is to explore whether SLAs, Providers, cloud models, cloud operational levels, threats, Virtualisation, organisational policy, governance, data life cycle, operating levels and legal issues have influence on cloud data security thus use them to design a security model for public institutions.

1.2 Problem Statement

As government parastatals (GPs) consider leaping from cloud computing as per vision 2030, they must also think about how to extend security to this new technology environment. Due to its projected cost savings, its elasticity, scalability and flexibility moving data and applications to the cloud is highly appealing. However, if the cloud service used is not sufficiently available, reliable, and secure, the business justification for moving to the cloud will be significantly reduced. And, unfortunately, the concentration of the data and applications in the cloud can create a more attractive target for potential attackers. There is need to look at the risks involved in moving to a cloud-based solution provider and ensure its security defences are appropriate for the business.

Cloud computing offers these public sector entities the opportunity to be more agile and innovative by consolidating, virtualizing and automating their ICT resources. (Macias and Greg, 2011) There are many concerns relating to the implementation of cloud computing such as Identification, authentication, Authorisation, Confidentiality, Integrity, Non-repudiation, Availability and among others.

A baseline survey of cloud computing in Kenya in 2013 reveals that security is one among other specific challenges hindering adoption of the cloud technologies in Kenya. One of the findings show that more organizations utilized pure private cloud (39%) compared to utilizing a public cloud (22%). The choice is more likely a result of concerns around security and control of access of organizational data. (Omwansa, Waema and Omwenga, 2014)

According to a study on cloud computing concerns on public sector conducted by Cisco in 2011, some of the issues that may arise when public sector organizations consider transitioning to cloud computing include Control and security. It explained that managers naturally want to determine how and where elements of the ICT system are deployed and used. Cloud computing raises a question of ownership and accountability within ICT groups, across the organization and extending to service providers and other vendors. Further, GPs must keep systems safe from intrusions, and they need to safeguard information, privacy, and, in the case of research institutions and universities, intellectual property. Security and privacy of data spans issues such as authentication, encryption, and detection of malware, side channel attacks and other kinds of attacks both internal and external to an institution.

This research focus is to provide a solution for cloud data security in GPs when they want to adopt cloud services for their work. For this purpose, a model will be designed for execution of data and information securely in cloud environment.

1.3 Research objectives

The research objectives have been broken down into the general and specific objectives with the specific objectives drawn from the general objectives.

1.3.1 General Objective

The primary aim of this research is to design a data security implementation model for cloud computing in Government parastatals.

1.3.2 Specific objectives

To analyze the service and deployment model implemented in government parastatals.

To analyze cloud computing security challenges and threats and techniques for protecting data in the cloud for government parastatals.

To investigate whether there exist other data security models in use in government parastatals.

To design a cloud data security implementation model in government parastatals.

1.3.3 Research questions

What are the service and deployment models implemented in government parastatals?

What are cloud computing security challenges, threats and techniques for protecting data in the cloud for government parastatals?

Are there other cloud data security models in use in government parastatals?

How can government parastatals go about implementing cloud data securely?

1.4 Justification

Security is a major concern among others in the adoption of cloud technologies. This has seen the public sector lag behind in the implementation of the cloud technologies. Since cloud computing involves migrating crucial resources such data, applications to a third party issues regarding privacy of data, control, management, access, ownership among others arise. Thus, many organizations in the public

sectors have concerns about using a cloud service provider. These concerns can be overcome if a risk-based approach is taken and appropriate security measures adopted. (Hp, 2013)

Among the three deployment models that is private, public and hybrid clouds, Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

In Kenya only a few organisations have migrated to the cloud and mainly private cloud. In order to increase adoption to the cloud technologies by the larger Kenya, the government should strongly welcome and support cloud computing technology to increase user confidence and accelerate adoption and exploitation.

Regulatory mechanisms need be sought to bring down the cost of entry into the business and reduce the cost to the end consumer. The ICT policy and legal frameworks should be reviewed to promote cloud computing and ensure that these frameworks are flexible and effective. The frameworks should create an enabling environment for organizations to invest in cloud systems, migrate their data and systems with ease and safety. Specific and targeted laws will help ensure the protection of end users particularly data protection, information security, privacy and cybercrime. (Omwansa, Waema and Omwenga, 2014)

A baseline survey of cloud computing in Kenya conducted in 2013 further recommends the following interventions. First, development of a national cloud strategy to focus on issues such as capacity building, architecture and implementation. Secondly, Government to champion cloud services by adopting use of the cloud to provide services and thus government would set pace for better uptake by the private sector and finally, Enhancement of relevant legal and regulatory frameworks for protection of cloud service users, addressing cyber security challenges, guaranteeing secure online payments, privacy and data security. The cloud data security model will help in increasing confidence in the adoption of cloud technologies, address cyber security challenges, enhance uptake of the cloud technologies in the larger Kenya, ensure privacy and data security in the public institutions.

1.5 Limitation of the Research

Public institutions are many in number. The researcher had conducted a preliminary to establish those that are IT enabled and have implemented cloud solution. There are procedures to follow in order to get information especially that related to security. These procedures could take a number of days to be approved.

It was difficult to identify those employees that have concrete information about the cloud and more specifically cloud security.

Undertaking data collection in these institutions proved to be costly and exhaustive. The study would limit itself to institutions within Nairobi and its environs.

The study requires staff in senior managerial position, middle level management and lower level position of the sample selected to fill in the questionnaire. The senior managers are difficult to catch due to their purported busy schedule. On the other hand cloud computing being relatively new the lower level staff have little or no information on the institutions progress on cloud computing. This can be attributed to the technicality of the paradigm, lack of training and poor communication structures between the top management and lower levels.

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

This chapter describes the theoretical and the conceptual frameworks. The theoretical framework looks into the available literature regarding the variables under investigation. The conceptual framework is a diagrammatical representation of how independent variables (i.e. platform, controls, service, cloud, policies, governance, data life cycle, level) influence the dependent variable (security).

2.1 Theoretical Framework

According to a study on cloud computing concerns on public sector conducted by Cisco in 2011 keeping data secure and personal information private is critical for any ICT implementation today, but particularly for those that serve large numbers of citizens. As ICT systems are extended and merged, there is growing fear that sensitive data that is collected and held by public entities will be vulnerable to criminal hackers or other types of unauthorized disclosure. This threat is magnified when a piece of crucial identity information, such as an ID number, can be linked to other information about that individual residing on the network, such as a financial or health record.

A security breach is inconvenient for individual users, but it can be a catastrophe for an organization whose reputation, credibility, and legal standing is at stake. Public sector organizations are especially vulnerable because their operations are tied so closely to the public's trust. When the relationship between organization and citizen is damaged, it is very difficult to repair. And lawsuits arising from assaults on privacy not only taint public perceptions, but can also deplete public funds.

There exists current research on detection and handling of security breaches to guard against tampering, loss and theft of data. Further, fault tolerant mechanisms for backing up data are required when there are failures in the infrastructure, such as net-work outages.

Many organizations in the public sectors have concerns about using a cloud service provider. These concerns can be overcome if a risk-based approach is taken and appropriate security measures adopted. (Hp, 2012)

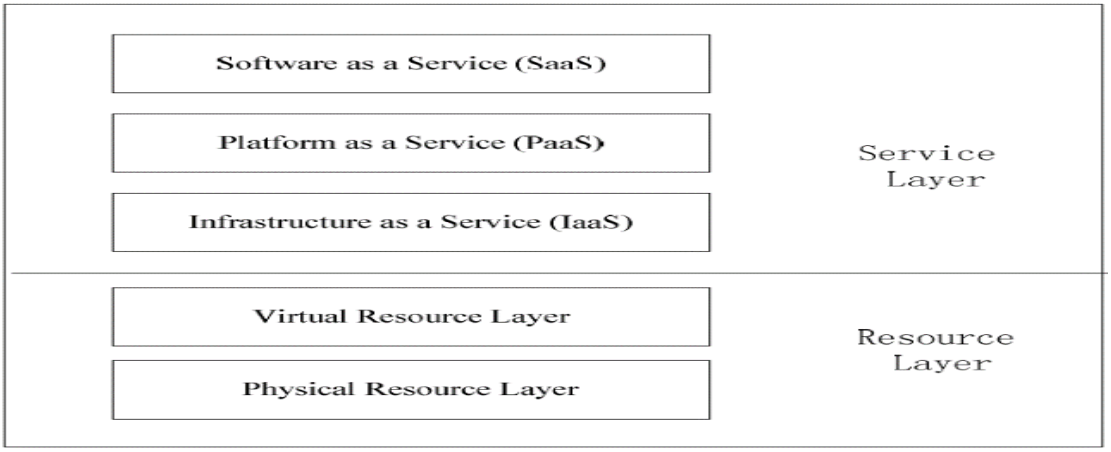
2.2 Cloud Computing

Cloud computing is arguably an emerging technology and is perceived to have many definitions, most of which focus on different aspects of cloud computing rather than provide a unified description (Vaquero et al., 2009). Cloud computing derives benefit from virtualization. Because, virtualization prevents complexity of hardware and software presentation by abstraction (allows to create an abstraction layer) such as storage virtualization which does this between the server side applications and the storage they use. At the bottom of the cloud computing architecture physical resources take place. Cloud computing uses the power of virtualization technologies in the virtual resource layer to virtualize systems which are constructed in the physical resource layer by pooling and sharing resources In other words, cloud computing gathers physical resources and presents them as virtual resources. It is characterized by virtualization, scalability and pay-per-use scalability model and resembles grid computing. The main aim of these two paradigms is to reduce costs and increase flexibility and reliability through the use of third party operated software. (Vaquero et al., 2009)Three different service models in the architecture are as follows: 1) Infrastructure as a Service (IaaS) 2) Platform as a Service (PaaS) 3) Software as a Service (SaaS).

2.2.0 Cloud Computing Service Models

Cloud computing architecture is needed to be examined in two different layers; one is the layer of resources and the other one is the layer of services. Resource layer is divided into two which are the physical resource layer and virtual resource layer.

Figure 2.1 Cloud computing architecture



Source: J. Xue and J. Zhang, (2010)"A brief survey on the security model of cloud computing.

According to (Dargha, 2011)Cloud services refer to those services that are exposed by a cloud vendor and that can be used by a consumer on a 'pay per use' basis. Three different service models provided in the architecture are classified as infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

i. Infrastructure as a service

IaaS is a provision model based on the need for equipment outsourcing to support daily operations. The entire computing infrastructure is provided as a 'service' by the cloud vendor. This service model provides virtual machines, virtual storage, virtual infrastructure database environment, a complete Linux environment and other hardware assets as resources. In this model, service provider is responsible for managing the entire infrastructure. On the other hand, some responsibilities exist for the clients which are operating system, applications and user interaction with the system. The responsibility of hosting and managing the infrastructure is with the vendor. Examples include Amazon EC2, Amazon simple DB and Amazon S.

ii. Platform as a service

PaaS can broadly be defined as application development environments offered as a 'service' by the vendors. It is a provision model based on the need for computing platform and solution stack. Provision of virtual machines, operating systems, development frameworks describes the goal of PaaS. Service provider responsibilities are managing cloud infrastructure, the operating system and enabling software. Clients responsibilities can be listed as application deployment or application use supported by PaaS, installing and managing the application. The development community can use these platforms to code their applications and then deploy the applications on the infrastructure provided by the cloud vendor. The responsibility of hosting and managing the required infrastructure is with the cloud vendor. Examples are Google App Engine, salesforce.com e.t.c

iii. Software as a service

SaaS is a software licensing and delivery model. This service model is a complete operating environment with applications, management and user interface. Applications like customer relationship management (CRM), Email, Instant messaging (IM), office productivity applications that are offered as a 'service' by a cloud vendor. In SaaS, service provider is responsible for hosting and managing everything from the application down to the infrastructure to support these services. Clients are responsible for entering and

managing its data and user interaction in this service model. The consumer of the service (an enterprise or an individual user) will use only those functionalities that they really want and pay for what they use.

2.2.1 Cloud Computing Deployment Models

(Ramgovind, Eloff and Smith, 2010) Observed that to provide a secure Cloud computing solution, it's important to decide on the type of cloud to be implemented. Currently there are three types of cloud deployment models offered, namely, a public, private and hybrid cloud.

a) Public Cloud

A public cloud is a model which allows users' access to the cloud via interfaces using mainstream web browsers. It's typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. This helps cloud clients to better match their IT expenditure at an operational level by decreasing its capital expenditure on IT infrastructure. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks. Therefore trust and privacy concerns are rife when dealing with Public clouds with the Cloud SLA at its core.

b) Private Cloud

A private cloud is set up within an organization's internal enterprise data centre. It is easier to align with security, compliance, and regulatory requirements, and provides more enterprise control over deployment and use. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud (Dooley, 2010)

c) Hybrid Cloud

A hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Clouds provide more secure control of the data

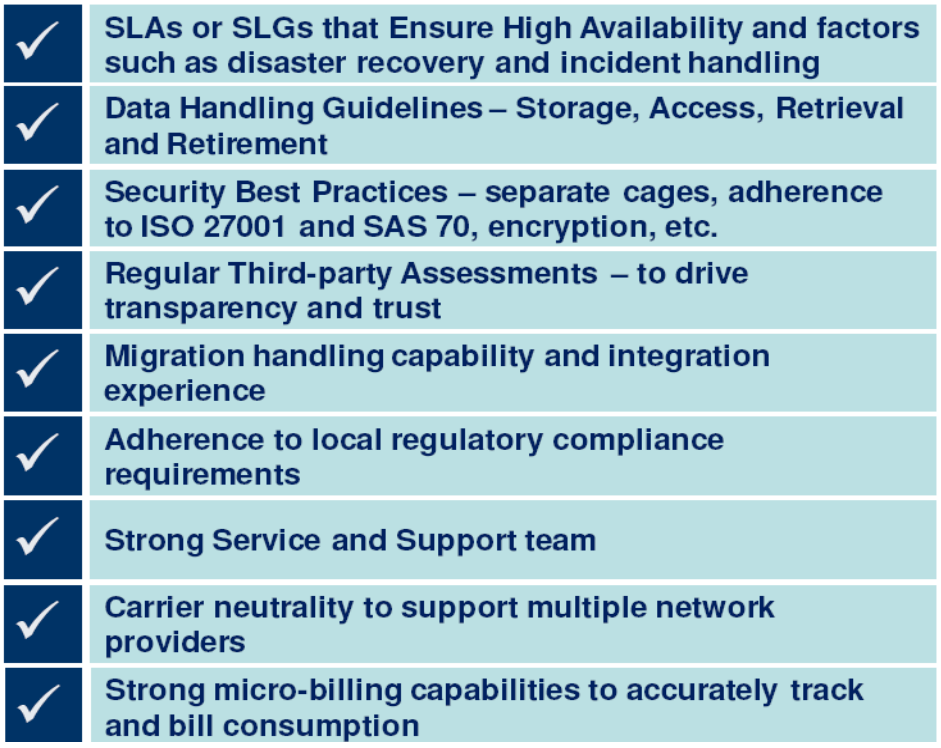
and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems (Ramgovind, Eloff and Smith, 2010)

To summaries, in the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand. In deciding which type of Cloud to deploy, business managers' needs to holistically assess the security considerations from an enterprise architectural point of view, taking into account the information security differences of each Cloud deployment model mentioned above.

2.2.2 Cloud Provider

Given the special considerations for government clouds, it is important for the public sector to consider various factors in selecting the right cloud service provider. It is essential to look beyond the cost savings of moving into the cloud to factors such as data centre location, security features, data handling policies and others. A checklist guide which may be useful in selecting the right federal cloud provider is illustrated below.

Figure 2.2: Checklist for Selecting the Right Federal Cloud Provider



Source: (Frost and Sullivan, 2010)Increasing Acceptance of Cloud Computing in the Public Sector

2.3 Cloud Security

Security is considered one of the most critical aspects in everyday computing, and it is no different for cloud computing due to the sensitivity and importance of data stored in the cloud (Alzain, Soh and Pardede, 2012). Cloud computing infrastructures use new technologies and services, most which haven't been fully evaluated with respect to security. Cloud computing security is a set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use. Wikipedia defines cloud security as a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. CSA (2011) explains that cloud security controls are not different from IT environment security. However, since cloud computing employs service models such as the operational models and the technologies used to enable cloud services cloud computing may present different risks to an organization than traditional IT solutions.

An organization security posture is characterized by maturity, effectiveness, and completeness of the risk adjusted security controls implemented. These controls are implemented in layers ranging from facilities (physical security), to network infrastructure (network security) and finally to applications and information (application security).

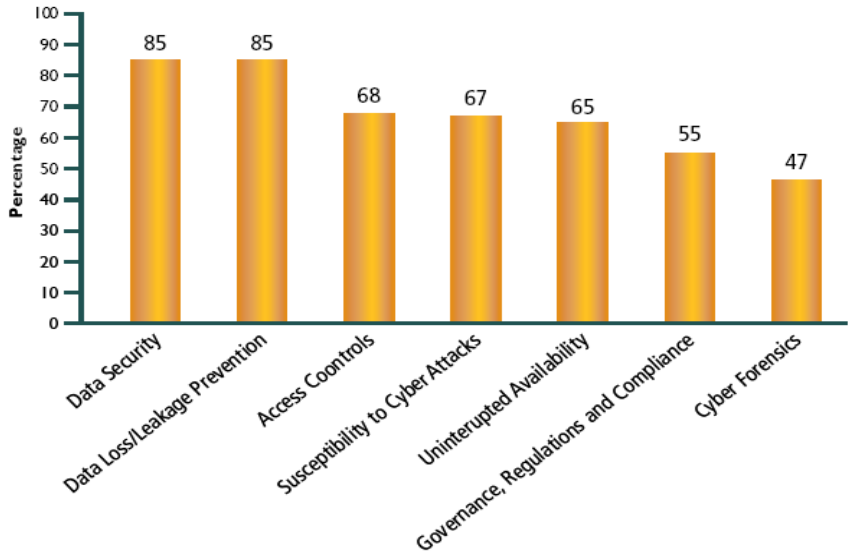
Yaser, Jennifer and Frank (2012) identify security and privacy as one of the challenges preventing adoption to cloud and advise that more research on this area. This category includes organizational and technical issues related to keeping cloud ser-vices at an acceptable level of information security and data privacy. This includes ensuring security and privacy of sensitive data held by banks, medical and research facilities. Security and privacy issues become even more serious when governmental institutions use the cloud. Despite the known need for Service Level Agreements between Cloud service providers and users, standards for safety have not yet been established and more research in this area would be beneficial. Security and privacy of data spans issues such as authentication encryption and detection of malware, side channel attacks and other kinds of attacks - both internal and external to an enterprise. There exists current research on detection and handling of security breaches to guard against tamper-in, loss and theft of data. Further, fault tolerant mechanisms for backing up data are required when there are failures in the infrastructure, such as net-work outages. The notion of using cloud resources as a utility has brought about a number of legal issues. The most discussed issue in the literature we surveyed is related to data placement. Laws and regulations vary widely across different regions and jurisdictions as to where and how data should be stored, processed, and used

Hashizume, Rosado and Fernadez-Medina (2013) explain that one of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters. Since Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved and how applications security is moved to Cloud Computing. That uncertainty has consistently led information executives to state that security is their number one concern with Cloud Computing Security concerns relates to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy and integration with internal security. Compared to traditional technologies, the cloud has many specific features, such as its large scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form. Security controls in Cloud Computing are not different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, Cloud Computing may present different risks to an organization than traditional IT solutions. Unfortunately, integrating security into these solutions is often perceived as making them more rigid.

2.3.1 Cloud computing security concerns

According to (Mano, 2011) many of the respondents of the 8th annual Global Information Security survey that was published in the CIO magazine have qualms about security, and more than 60 percent of the respondents admitted to having little to no confidence in the ability to secure assets that are placed in the cloud .The findings of the (ISC)2 GISWS highlight seven security concerns as shown.

Figure 2.3 Security Concerns in Cloud Computing "Cloud computing: Opportunity or Crisis?"



To facilitate further studies (Gonzalez et al., 2012) organizes the information related to cloud security. The main problems are identified and grouped into a model composed of seven categories: network security, interfaces, data security, virtualization, governance, compliance and legal issues.

Several key references were employed to gather the information required for building these categories, including CSA's security guidance and top threats analysis, ENISA's security assessment and the cloud computing definitions from NIST. Emphasis is given on the distinction between services in software (SaaS), platform (PaaS) and infrastructure (IaaS), which are commonly used as the fundamental basis for cloud service classification. Each category includes several potential security problems, resulting in the classification with subdivisions that highlight the main issues identified by the aforementioned references: 1) Network security: Problems associated with network communications and configurations regarding cloud computing infrastructures. The ideal network security solution is having cloud services as an extension of customer's existing internal networks, adopting the same protection measures and security precautions that are locally implemented and allowing extending local strategies to any remote resources or processes such as Transfer security, Firewalling and Security. 2) Interfaces: Concentrates all issues related to user, administrative and programming interfaces for using and controlling clouds. They include API: Administrative interface, User interface and Authentication. 3) Data security: Protection of data in terms of confidentiality, availability and integrity (which can be applied not only to cloud environments, but any solution which requires basic security levels). They include Cryptography, Redundancy and Disposal. 4) Virtualization: Isolation between VMs, hypervisor vulnerabilities and other problems

associated to the use of virtualization technologies. They include Isolation, Hypervisor vulnerabilities (The hypervisor is the main software component of virtualization. Even though there are known security vulnerabilities for hypervisors, solutions are still scarce and often proprietary, demanding further studies to harden these security aspects).5) Governance: Issues related to (losing) administrative and security controls in cloud computing solutions. They include a) Data control, Security control and Lock-in. 6) Compliance: Category which includes requirements related to service availability and audit capabilities. They include Service Level Agreements (SLA), Loss of service and Audit. 7) Legal issues: Juridical concerns related to new concepts introduced by cloud computing such as multiple data locations and privilege management. They include: Data location, E-discovery and Provider.

Table 2.1: Cloud Computing Security Concerns, Threats and Controls

Data Security	Disclosure to unauthorized systems or personnel	Cryptographic protection such as encryption or hashing of sensitive / privacy data Cryptographically agile applications.
Data Loss/Leakage Prevention	Data loss/leakage and data eminence	Secure data disposal Overwriting (formatting) of storage media.
Data classification and labelling	Data Loss/Leakage Prevention (DLP) technologies	Access Controls Unauthorized access, access control lists (ACLs) Chinese Wall Hardening Abuse and Nefarious Use of Computing Resources
Cracking	Malware	Stronger authentication mechanisms Secure transmissions (tunnelling) Hardened infrastructure, platforms and applications
Insecure and Proprietary APIs	Clear text authentication Inflexible access control Limited monitoring and auditing	Understand the dependency chain of APIs Deprecate insecure APIs Perform ROI exercise for proprietary APIs

	Vendor lock-in	
Shared Technology Vulnerabilities Hypervisor exploits	Cloud bursting	Sandboxing and Hardening Resource planning and provisioning Defence-in-depth
Hijacking of Accounts, Services and Traffic	Disclosure to unauthorized systems or personnel	Session management Secure transmissions (tunnelling)
Provider's Risk Profile Unknown	Provider's inner workings Processes and procedures are a black box	Periodically assess provider's risk profile Verify and validate provider's assurance controls claims
Uninterrupted Availability	Denial of Service (DoS) Distributed Denial of Service (DDoS) Uptime uncertainty	Capacity planning Redundancy and Backup Performance and Uptime requirements in Service Level Agreements (SLA)
Governance, Regulations and Compliance	Uncertainty in enforcing security policies at provider's site Inability to support compliance audits	Establish contracts that are enforceable Periodically assess provider's risk profile Verify and validate provider's assurance controls claim
Cyber Forensics	Collection of evidence in a dynamically provisioned environment is a challenge Lack of understanding of provider's infrastructure to collect evidence successfully	Visualization of physical and logical data locations Cryptographically agile applications
Personnel Security	Malicious Insider Insider attacks	Identity management with auditing to assure non-repudiation Background screening checks Awareness, Training and Education

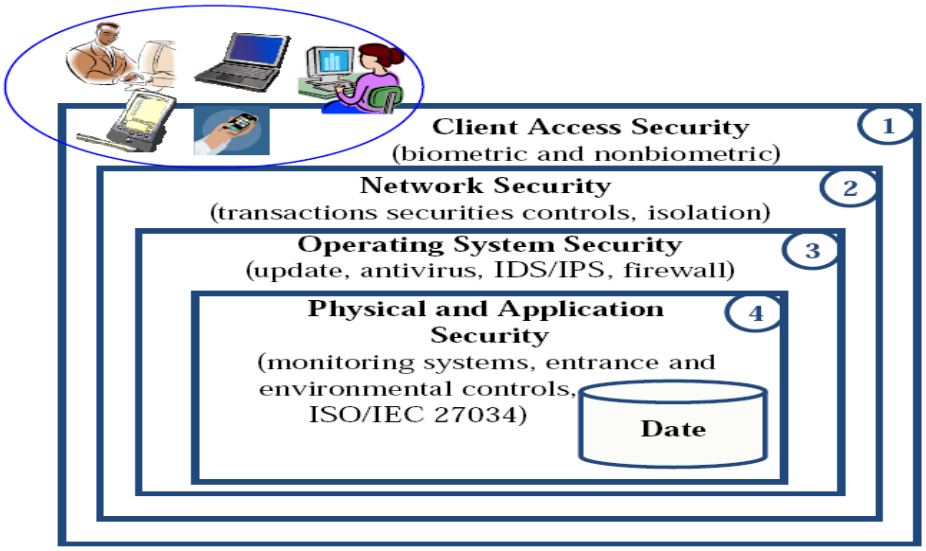
Source: (CSA, 2011)Security guidance for critical areas of focus in cloud computing v3.0

2.3.2 Data Security Risks in the Cloud

To ensure data security in the cloud (Mircea, 2012) indicates that it requires the identification and analysis of the risks and security measures/techniques that can be applied in every stage of data life cycle. The omission of one of the stages, at least in the case of the sensitive data for organization, may lead to important loss for the organization. (Mircea, 2012) Identifies some examples of data security risks in the cloud, categorized according to the stages of data life cycle namely: create, store, share, use, maintain and destroy.

The use of cloud computing involves certain changes in the traditional methods of data security. These are mainly determined by cloud-based architectures that lead to multitenancy and geographic diversity. The data security along their life cycle may be achieved on different levels as indicated in the figure below. On every security level there may be applied different techniques/methods that would ensure the compliance of the security policy established at organization level. The data access will be achieved by following one or several security.

Figure 2.4 Levels according to the requirements established through the security policy.



Source: Addressing Data Security in the Cloud. World Academy of Science, Engineering and Technology Vol: 66 2012-06-28 pg508)

2.3.3 Data Security Assessment in the Cloud

According to (Mircea, 2012) Security assessment helps in determining the system's capacity of responding to potential exposures and incidents. It also helps the organization in identifying the deviations between the proposed security strategies and the actual state of the security system. The assessment represents the foundation in determining the potential losses and the premise in the subsequent security improvement.

The methods of security assessment include the international standards (for instance, ISO/IEC 27002:2005, NIST's SP800-53) as well as efficient practiced developed by security organizations, such as Cloud Security Alliance

(CSA), European Network and Information Security Agency (ENISA), Information Systems Audit and Control Association (ISACA) and the Payment Card Industry (PCI). Moreover, in recent years efforts were made in ensuring Security, such as CERT's OCTAVE, Cloud Audit (A6), and Open Cloud Computing Interface (OCCI). The Cloud Security Alliance suggests in "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1" that they must offer guides in selecting cloud services providers; they must include small and medium enterprise security in the contractual obligations; they must analyze the changes in security metrics by passing to cloud, and they must include metrics and security standards in any SLAs and contracts. The assessment of data security in the cloud must be performed for all types of data in the most important areas of the business. In order to be successful, the security assessment process must involve staff from the following departments: human resources, corporate legal, audit, risk management, IT security, physical security, organization security and other business units. The assessment must also be connected to the other stages of the life cycle of the security insurance process, in order to implement the results and to obtain real advantages

2.3.4 Cloud security models

Security is a major concern in cloud computing. There are many different reference models and standards that apply to a security Software or solution or system Development Life Cycle (SDLC). (Wrinkler, 2011) Explains some of the models that can serve as reference models for security engineering, security architecture, security operations, and certainly for cloud security. But doing so is not always straightforward, as some of these are proprietary or controlled by a single entity. Furthermore, not all of the existing reference models have security architecture or security controls as their focus. (Wrinkler, 2011)) describes some of these models as follows: 1) ISO 27001 through ISO 27006. This series of international standards for information security covers: management, best practices, requirements, and techniques. These have important value in their potential applicability to cloud computing security. 2) European Network and Information Security Agency (ENISA) it is the European cyber security agency. In 2009, ENISA published a Cloud Computing Information Assurance Framework which heavily adopts ISO 27001 and 27002 controls for cloud computing. In the same year, ENISA also published Cloud Computing Benefits, Risks and Recommendations for Information Security. Together, these documents offer background on the security issues for organizations wishing to adopt cloud computing. 3) Information Technology Infrastructure Library (ITIL). Core to ITIL is the understanding that IT services must be aligned to business needs. Focused on IT service management, ITIL defines processes that are structured around service life cycles and practices. Security management in ITIL is based on ISO/IEC 27002. ITIL offers indirect value beyond IT service management in planning and architecture phases. 3) Control Objectives for Information and related Technology (COBIT) is a framework for IT management that was developed by the Information Systems Audit and Control (ISACA), along with the IT Governance Institute. It is a set of generally accepted best practices, measures, and indicators for IT governance and control. COBIT is broader in scope than ISO/IEC 27002, which is focused on security. Future development proposes generation of Governance, Risk Management, and Compliance (GRC) platforms in the cloud. These platforms will be used to check compliance in both cloud applications, as well as internal deployments. GRC platforms can lessen an IT organization's burden of developing a governance package, as well as developing auditing initiatives. The

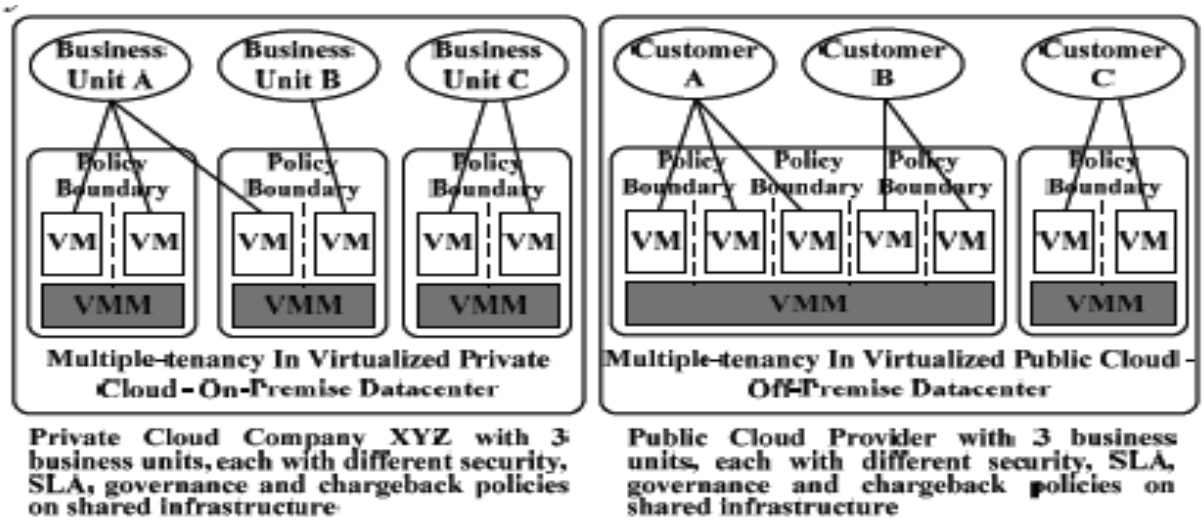
development of cloud GRC platforms allows a company to use a third party GRC application to audit another third party cloud computing environment. Cloud computing environments will sign up for the third party audit to demonstrate to clients that they meet certain Governance, Risk levels and Compliance levels.

(Ritesh, Chatur and Swati, 2012) further elaborates popular security models of cloud computing, such as multiple-tenancy model, risk accumulation model as follows.

2.3.5 The Cloud Multiple-Tenancy Model of NIST

Multiple-tenancy is an important function characteristic of cloud computing that allows multiple applications of cloud service providers currently running in a physical server to offer cloud service for customers. This physical server partitions and processes different customer demands with virtualization. Virtualization possesses good capability of sharing and isolation, and is a right core technology of cloud computing. By running multiple virtual machines (VMs) in a physical machine, virtualization enables to share computing resource such as processor, memory, storage, and I/O among different customers‟ applications, and improves the utilization of cloud resources. By hosting different customers‟ applications into different virtual machines, virtualization enables to isolate fault, virus, and intrusion of one from other virtual machines and hardware, and reduce the damage of malicious applications. The technology difficulties of multiple-tenancy model include data isolation, architecture extension, configuration self-definition, and performance customization. Data isolation means that the business data of multiple customers do not intervene mutually. Architecture extension means that multiple-tenancy should provide a basic framework to implement high flexibility and scalability. Configuration self definition means that cloud computing should support different customers‟ respective demands on its service platform configuration. Performance customization means that cloud computing should assure different customers‟ demands on the performance of multiple-tenancy platform under different workload. The impact of multiple-tenancy model is different corresponding to different cloud deployment models. Taking SaaS as an example, SaaS with multiple-tenancy function characteristic has two basic features. First, it is easy to scale-out and scale-up to serve for a mass of customers based on Web service. Second, it can present additional business logic that enables customers to extend its service platform and satisfy larger enterprises‟ demands. Multiple-tenancy model of cloud computing implemented by virtualization offers a method to satisfy different customer demands on security, segmentation, isolation, governance, SLA and billing/chargeback etc.

Figure 2.6 Cloud Multiple-Tenancy Model of NIST.



Source: International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012 Cloud Computing and Security Models: A Survey

2.3.6 The Cloud Risk Accumulation Model of CSA

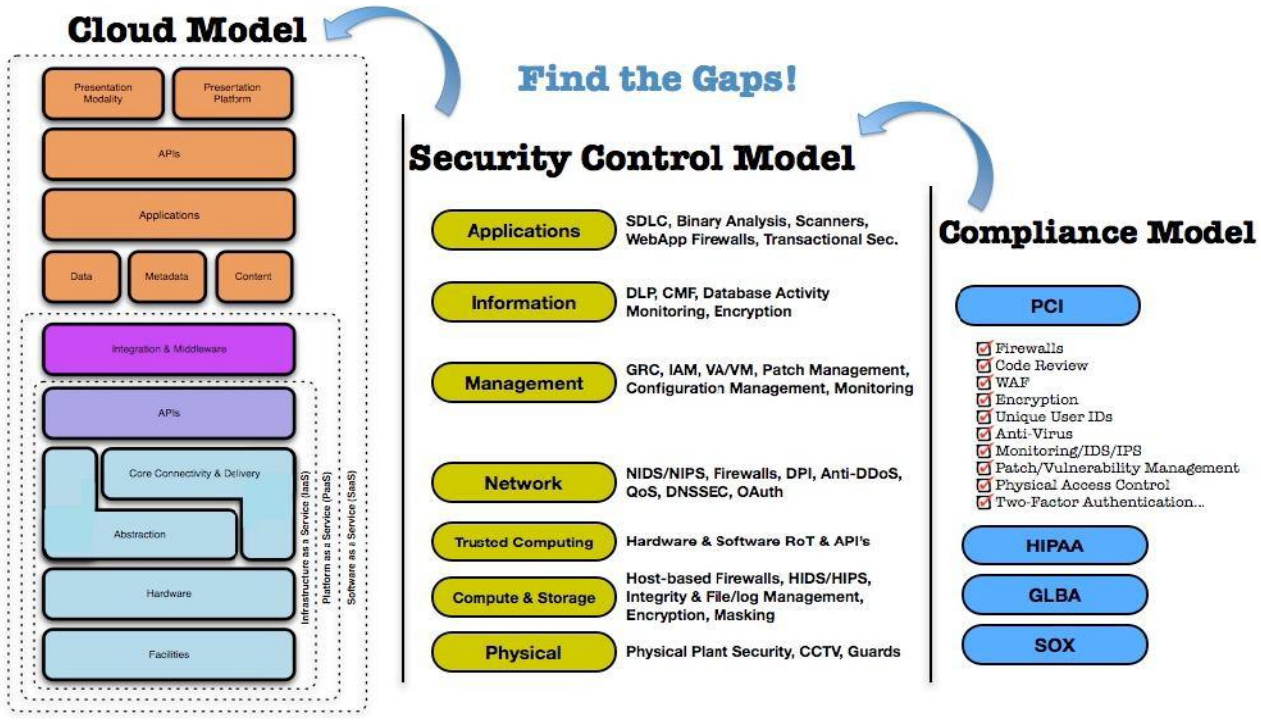
Understanding the layer dependency of cloud service models is very critical to analyze the security risks of cloud computing. IaaS is the foundation layer of all cloud services, PaaS is built upon IaaS and SaaS is built upon PaaS, so there is an inherited relation between the service capability of different layers in cloud computing. Similar to the inheritance of cloud service capability, the security risks of cloud computing is also inherited between different service layers • IaaS provides no distinctive function similar to application service but maximum extensibility for customers, meaning that IaaS holds little security functions and capabilities except for the infrastructure's own security functions and capabilities. IaaS demands that customers take charge of the security of operating systems, software applications and contents etc. • PaaS offers the capability of developing customized applications based on the PaaS platform for customers and more extensibility than SaaS, at the cost of reducing those available distinctive functions of SaaS. Similarly, the intrinsic security function and capability of PaaS are not complete, but customers possess more flexibility to implement additional security. • SaaS presents the least customer extensibility, but the most integrated service and the highest integrated security among three service layers. In SaaS, cloud service providers take charge of more security responsibilities, and customers pay for little security effort on the SaaS platform. One critical feature of cloud security architecture is that the lower service layer that a cloud service provider lies in, the more management

duties and security capabilities that a customer is in charge of. In SaaS, cloud service providers need to satisfy the demands on SLA, security, monitor, compliance and duty expectation etc. In PaaS and IaaS, the above demands are charged by customers, and cloud service provider is only responsible for the availability and security of elementary services such as infrastructure component and underlying platform.

2.3.7 The mapping model of cloud, security and compliance

The mapping model of cloud ontology, security control and compliance check presents a good method to analyze the gaps between cloud architecture and compliance framework and the corresponding security control strategies that should be provided by cloud service providers, customers or third parties .To protect effectively the security of cloud environment, we should firstly analyze the security risks confronted by cloud environment, and then find out the gap matrix according to cloud architecture and its compliance framework, and finally adopt some relevant security controls. Here, the compliance framework of cloud computing is not naturally existed with the cloud model. Correspondingly, the mapping model of cloud, security and compliance contributes to determining whether accept or refuse the security risks of cloud computing.

Figure 2.7: The mapping model of cloud, security and compliance



Source: International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012 Cloud Computing and Security Models: A Survey

2.3.7 Standardization and Legal Concern

Due to the nature of cloud computing, combining existing technologies and presenting differently, various standards can be applied in this field. It is too hard to construct a big picture which can be a standard or act as a suggestion. Instead, there are many of them that focus on specific parts of cloud computing. Field of IT has some difficulties such as non standard material usage and impalpable processes. Cloud computing inherits these difficulties also adds new ones onto them. Therefore, understanding the gravity of communities for pooling best practices and gathering stakeholders are musts in this era of information.

An eye catching structure comes with Open Virtualization Format (OVF). Deployment-platform free characteristic of OVF should count as an advantage because of different virtualization platforms. On the other hand, secure service provisioning is another critical subject for cloud computing. Information Technology Infrastructure Library (ITIL) and ISO/IEC 27001/27002 are such examples which focus on ensuring secure service provisioning. Communities like Cloud Security Alliance (CSA) allow non-profit organizations and individuals to enter into discussion. Thus, they become a part of solution itself (Popovic and Hocenski, 2010)

Because of cloud computing nature of combining and presenting several type services under one roof, examination of current regulations clearly shows that there is an incompetency on privacy protection according to the following issues (Cheng and Lai, 2012): 1) Under certain circumstances, service providers are obliged to disclose customers' information in United States. This is permitted by "The Stored Communications Act" legislation. According to the same legislation service provider type is unimportant which is electronic communication service provider or remote computing service provider. 2) The problem here is cloud computing service providers may be qualified either as an electronic communication service provider or a remote computing service provider. Therefore, a legal misuse may be observed by utilizing this gap.

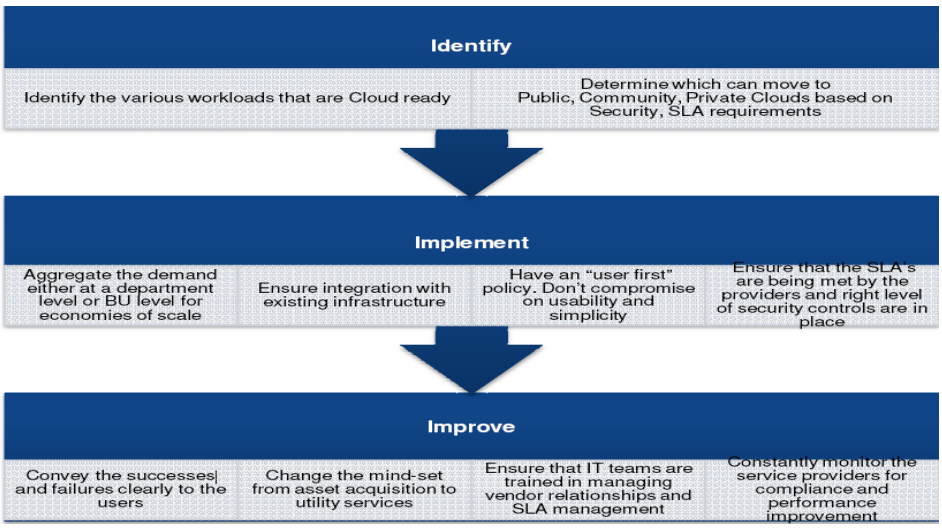
Information privacy protection in European Community seems to have more solid ground than United States because of the following reasons (Cheng and Lai, 2012): i) In Directive 95/46/EC there is a manifest which includes a personal data disclosure that racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex must be protected with certain exceptions. ii) Public electronic communications networks and services including telecom operators, mobile phone communication service providers, internet access providers, providers of the

transmission of digital TV content, and other providers of electronic communication services that are offered to the public are bound to provide the notification of information security breach through Directive 2002/58/EC. In other words, service providers have to assure the information security breach report for any accident which is expected from related authorities. iii) There is an article in 95/46/EC states restrictions for transfer of personal data outside the European Community.

iv. Framework for Cloud Migration

Migrating to cloud often involves a mammoth evaluation exercise that looks at the readiness of applications and data and the business case for doing so. While the challenges in the government sector are no different from that of the private sector, the issues of procurement and security are more pronounced in this sector. The government has an onus to protect citizen data and ensure high availability of the critical national infrastructure such as power, water, health, communications, and banking. Budgeting in the government sector works much differently from that of the private sector. IT budgets are planned well in advance, often a few years before, leaving agencies with little flexibility for last minute changes. Selection of vendors/service providers is a long drawn process that strives to minimize the suppliers and procure services at a lower price. Due to the nature of the process, the government runs a risk of being unable to procure IT services from niche service providers that can deliver innovative services at low prices. Hence, it is very important for government agencies to change the traditional procurement models if they are serious about procuring ICT resources from the cloud. The following chart provides a basic framework for agencies looking to migrate to cloud. (Frost and Sullivan, 2010)

Figure 2.8: Cloud Migration Framework



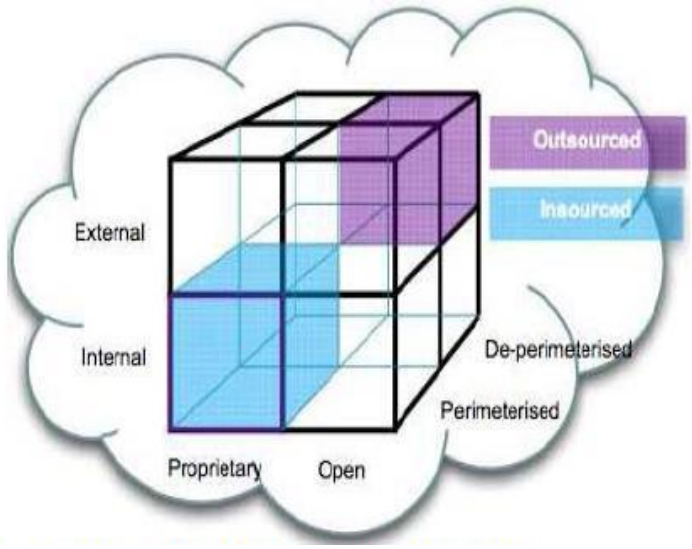
Source: Frost and Sullivan (2010) Increasing Acceptance of Cloud Computing in the Public Sector

2.3.9 Jericho Forum's Cloud Cube Model

Jericho forum's cloud cube model is a figuration description of security attribute information implied in the service and deployment models of cloud computing and the location, manager and owner of computing resources and so on as figure 3 shown. In cloud cube model, the definitions of model parameters are as follows:

Internal/External: a model parameter to define the physical location of data storage. If the physical location of data storage is inside of the data owner's boundary, then the model parameter value is internal. Contrariwise, the model parameter value is external. For example, the data centre of a private enterprise cloud is internal, and the data centre of Amazon's SC3 is external. Note: the cloud with internal data storage is not more secure than the one with external data storage. The combination of internal and external data storage maybe present more secure usage model. **Proprietary/Open**: a model parameter to define the ownership of cloud's technology, service and interface etc. This model parameter indicates the degree of interoperability, i.e. the portability of data and application between proprietary system and other cloud modalities, the ability of transforming data from a cloud modality to other cloud modality without any constraint. Proprietary means that a cloud service provider holds the ownership of facilities providing cloud services, hence the operation of cloud is proprietary and customers can not transfer their applications from one to another cloud service provider without great effort or investment. The technologies used in public cloud are generally open and uniform, meaning more available service providers and less constraint on data share and incorporation with business partners. Unproven but most, open clouds can promote effectively the incorporation between multiple organizations. **Perimeterised/De-perimeterised**: a model parameter to describe the "architectural mindset" of security protection, i.e. a customer's application is inside or outside of traditional security boundary? Perimeterised means that a customer's application operates within traditional IT security boundary signalled by firewall that blocks the incorporation of different security zones. In fact, customers running some applications inside of security zone can extend/shrink their application perimeter to/back from external cloud environment by VPN. De-perimeterised means that the fade way of traditional IT security boundary and the exposure of a customer's application operation. For the security protection of deperimeterised environment, Jericho Forum uses the meta-data and mechanisms in their commandments and Collaboration Oriented Architectures Framework (COA) to encapsulate a customer's data. **Insourced/Outsourced**: a model parameter to define the 4th dimension that has two states in each of the eight cloud forms: Per(IP,IO,EP,EO) and D-p(IP,IO,EP,EO). Insourced means that cloud service is presented by an organization's own employees, and Outsourced means that cloud service is presented by a third party. These two states answer the question "who do you want to build or manage your cloud

service?" This is a policy issue (i.e. a business but not a technical or architectural decision).In cloud cube model, other attributes such as Offshore and Onshore are also relevant to cloud computing, but in this paper we have focused on the four dimensions identified in cloud cube model.



2.3.10 Multi-Clouds Database Model

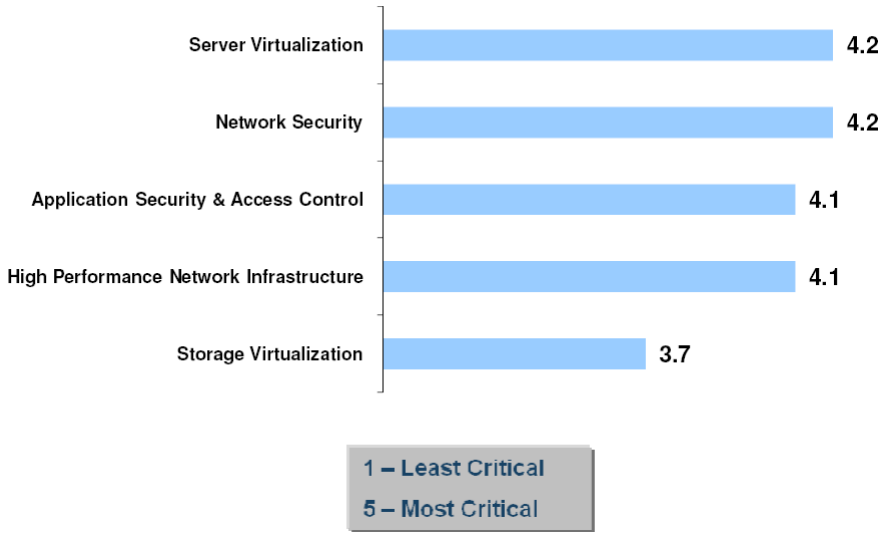
Multi-Clouds Database Model presents cloud with database storage in multiclouds service provider. MCDB model does not safeguard security by single cloud; rather security and privacy of data will be provided by implementing multi shares technique on multi-cloud providers. By doing so, it lessens the negative effects of single cloud, reduces the security risks from malicious insider in cloud computing environment, and narrows the negative impact of encryption techniques.

MCDB provides security and privacy of user's data by replicating data among several clouds and by using the secret sharing approach. It deals with the database management system (data source) to manage and control the operations between the clients and the cloud service providers (CSP). At the client side, this sends data inquiries to server or instance such as in Amazon in CSP. The data source stores the data in the cloud side which is supposed to be a trusted cloud, additional to ensuring the privacy of any query that the client has made and for the security of the client stored data. A problem occurs when we cannot guarantee cloud is a trusted service.

2.3.11 Critical ICT Components in Building a Cloud

While putting together a cloud, it is essential to understand the different components that are essential to build and maintain a cloud that performs as per government requirements. According to a recent Frost & Sullivan study in the Asia Pacific region, governments have allocated highest priority to server virtualization and network security. Server virtualization will help governments meet their resource consolidation objectives. Furthermore, security is paramount to government adoption. Governments will adopt cloud computing only if they are convinced that their data will remain secure and available. (Frost and Sullivan, 2010)

Figure 2.9: Illustrates the priority attached to different ICT components in building a cloud.

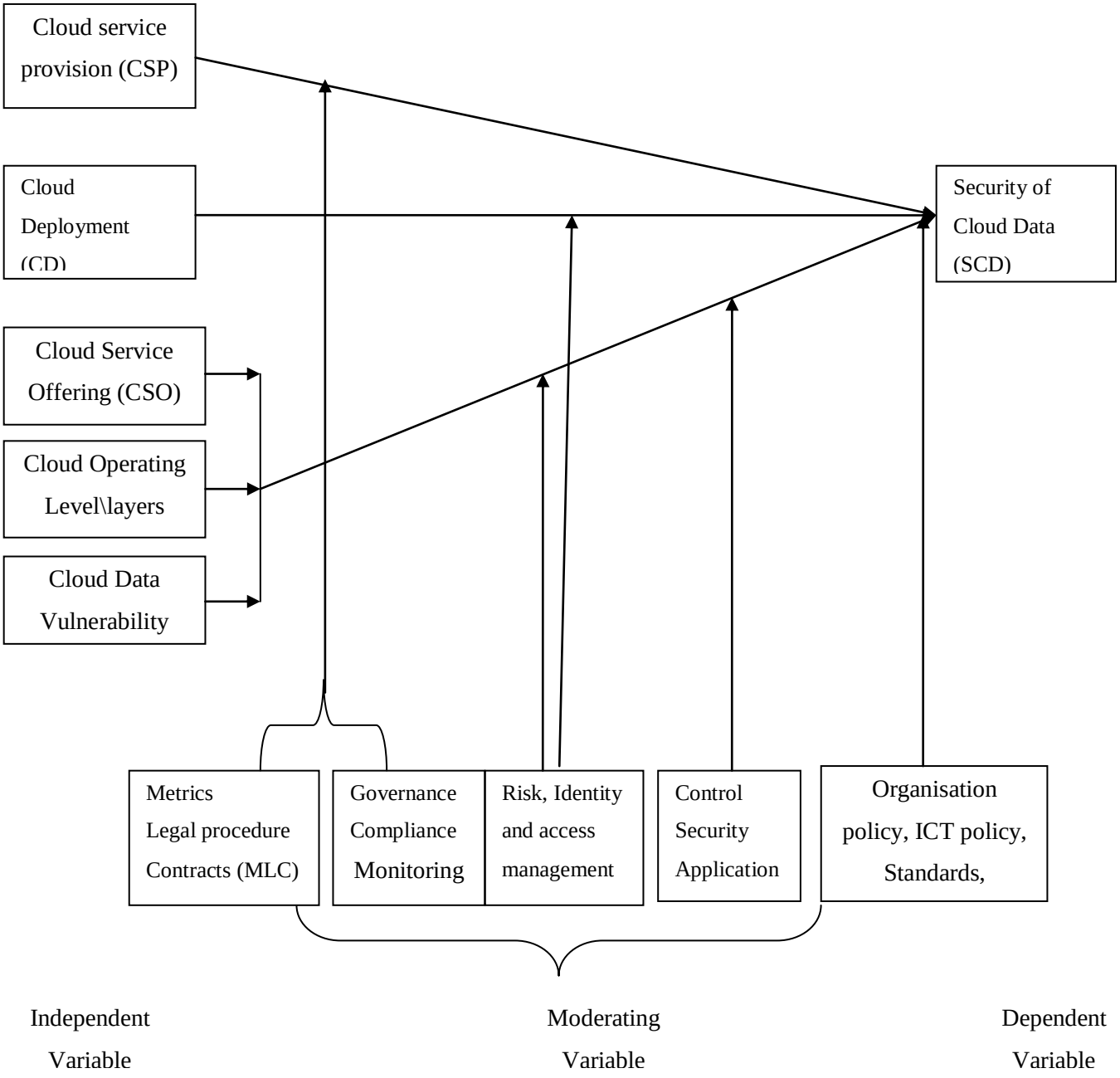


Source: Frost and Sullivan (2010) Increasing Acceptance of Cloud Computing in the Public Sector

2.4 Conceptual Framework

From the literature review, different types of clouds have different security levels. According to cloud risk accumulation model of CSA understanding layer dependency on cloud service models helps in analyzing risks of cloud computing. This study will investigate how Cloud Service Provision(CSP), Cloud deployment(CD), Cloud Service Offering (CSO), Cloud operating Layer/level(COL), cloud Data Vulnerabilities(CDV) through the moderating variables represented in figure 2.10 affect the cloud data security implementation in government parastatals.

Figure 2.10 Conceptual framework



2.4.1 Cloud Service Provision (CSP)

CSP provide services. CSP controls most aspects of the service offering such as location, access, security features, policies, compliance, capacity, profile risk and many others. This research will analyse the effect of CSP on the security of the cloud data in GPs.

2.4.2 Cloud Deployment (CD)

Security has always been a major concern in relation to deployment models. Different deployment models have different security requirements and features. For instance, private clouds are perceived to be more secure than public clouds. This research will analyse the effect of CD on the security of cloud data in GPs.

2.4.3 Cloud Service Offering (CSO)

CSO entails cloud service models offered to the cloud clients for instance SaaS, IaaS and PaaS. There exist relationships and dependencies between these cloud service models that may affect security of data in the cloud. PaaS as well as SaaS are hosted on top of IaaS; thus, any breach in IaaS will impact the security of both PaaS and SaaS services, but also it may be true on the other way around. However, we have to take into account that PaaS offers a platform to build and deploy SaaS applications, which increases the security dependency between them. As a consequence of these deep dependencies, any attack to any cloud service layer can compromise the upper layers. Each cloud service model comprises its own inherent security flaws; however, they also share some challenges that affect all of them. These relationships and dependencies between cloud models may also be a source of security risks. A SaaS provider may rent a development environment from a PaaS provider, which might also rent an infrastructure from an IaaS provider. Each provider is responsible for securing his own services, which may result in an inconsistent combination of security models. It also creates confusion over which service provider is responsible once an attack happens. This research will analyse the effect of CSO on the security of cloud data in GPs.

2.4.4 Cloud Operating Layer/Level (COL)

An organisation's security posture is characterized by the maturity, effectiveness, and completeness of the risk-adjusted security controls implemented. These controls are implemented in one or more layers ranging from the facilities (physical security), to the network infrastructure (network security), to the IT systems (system security), and all the way to the information and applications (application security). This research will analyse the effect of COL on the security of cloud data in GPs.

2.4.4 Cloud Data Vulnerabilities (CDV)

Security is about reducing chances of the cloud vulnerabilities such as a malware, DoS, hypervisor vulnerabilities, data loss, administrative issues such as unauthorised access, security controls loss, loss of service availability, data lock-in, jurisdiction concerns such as multiple locations. New security

techniques are needed as well as redesigned traditional solutions that can work with cloud architectures. This research will analyse the effect of CD on the security of cloud data in GPs.

The independent variables are influenced by

2.4.5 Metrics, legal issues and contracts (MLC)

It Cloud computing provides metrics for the services used. Such metrics are at the core of the public cloud pay-per-use models. Data Security metrics are designed to show the effectiveness of the organization's controls to ensure the confidentiality, integrity, and availability of sensitive data. These metrics should measure the levels of protection of sensitive data while at rest, in use, and in motion. MLC influences CSP greatly. Metrics ensure SCD is not compromised. The cloud client has to have metrics employed to gauge the CSP ensure legal and obligations are met and contractual agreements met. This research will analyse how MLC influences CSP towards the security of cloud data in GPs.

2.4.6 Governance compliance and monitoring (GCM)

GCM involves governance, compliance and monitoring. Governance entails planning, risk management and auditing. Most cloud clients forego governance which is a very critical aspect in ensuring that CSP is smooth thus reducing the chances of security breaches n the SCD. It involves employing administrative and security policies and controls in cloud solutions, monitoring and ensuring full compliance by the CSP to ensure SCD. This research will analyse how GCM influences CSP towards the security of cloud data in GPs.

2.4.7 Risk management, identity and access management (RIAm)

Risk management, identity and access management involves clients conducting a thorough risk analysis in cloud deployments(CD), cloud service offering(CSO), cloud operating level/layers(COL), and cloud data vulnerabilities(CDV) repercussions. Its critical that cloud clients understand their level of risk tolerance and focus on the mitigating risks that the organisation cannot afford to neglect.

Identity and access control mechanisms encompasses mechanism which allow managers to permit, direct or restrain not only content but user behaviour / use of a system. Loopholes in any of these expose systems to cloud data vulnerabilities and exploitation. This research will analyse how RIAm influences CD, CSO, COL and CDV towards ensuring security of cloud data in GPs.

2.4.8 Control and security application (CSa)

Control and security application influences cloud service offering (CSO), cloud operating layers (COL) and cloud data vulnerabilities (CDV) in that the CSP should ensure administrative and security control for every service model taking into account inherent dependences and challenges among service models.

Security of cloud data (SCD) is characterised by maturity, effectiveness, completeness of the risk adjusted security controls implemented. These controls are implemented on every cloud operating layer (COL). This reduces cloud data vulnerabilities (CDV) levels and thus ensuring SCD. This research will analyse how CSa influences CSO, COL and CDV towards ensuring security of cloud data in GPs.

2.4.9 Policies, standards and regulations (PSR)

PSR entails organisation and ICT policies, standards and regulations form the basis for governance and management. It involves developing policies to govern cloud solution, setting up standards by relevant bodies to standardise implementation of cloud technology, enacting laws that would regulate cloud service offerings and provisions ensuring level playing field for all stakeholders. This research will analyse how PSR influences all aspects of the framework towards ensuring security of cloud data in GPs.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

One of the most common and important aspect in any research is collection of data. Different methods of data collection such as interviews, surveys, field notes, questionnaires, focus groups and many others can be used. This chapter covers research design, sample population, data collection techniques and analysis. The main aim of this section is to provide a solution to how government parastatals can implement their data securely in the cloud. It describes the research design to be used and explains why the descriptive research design was seen as the most appropriate. The chapter explains why sample study methodology was adopted for the research. The section describes in depth the techniques applied to collect data. The proposed model will be used for analysis, validation and reliability. Finally the challenges faced by opting to use the data collection techniques and the research methodology used.

3.2 Research Design

The research design refers to a strategy used by the researcher in collecting and analyzing data in order to answer the research questions or test the research hypothesis (Kerlinger, 1986). The research design to be adopted is a descriptive survey aimed at investigating how government parastatals can go about implementing data securely and whether there exists cloud data model in use. Cloud computing is a relatively new technology in the IT industry thus only few private and public organizations have fully migrated their data and resources. However literature shows that the uptake is increasing though gradually.

After careful evaluation of the literature, descriptive design was found to be most appropriate since it will ensure the description of the state of affairs, as it exists at present in government parastatals.

One of the most time-honoured approaches to investigating important information systems and organisational phenomena is quantitative research (also known as quantitative, positivist research - QPR). Quantitative techniques have been used so often and for so long that a set of standards as to what is acceptable have emerged and are generally expected by knowledgeable reviewers (Avison and Heje, 2005).

The researcher mainly used questionnaires as data collection instruments. Two formats of the questionnaire. As presented in appendix II and III respectively were designed a) online questionnaire created using Google forms were sent to ICT staff who were away from their working place at the time. Online responses were received via Email. b) Hardcopy questionnaire which were circulated personally by the researcher to the various organisations and filled questionnaires were collected after a few days

The data was collected and analyzed to provide information used to describe and interpret current events. It will also be useful in studying the inter-relations between the variables already mentioned in the conceptual framework. The variables are known and well defined. This design was adopted, as it allows collection of large amounts of data from the target population. Indeed, QPR allows information systems researchers to answer scholarly and pragmatic questions about the interaction of humans and artifacts such as computers, systems and applications (Avison and Heje, 2005).

A preliminary study of government parastatals with cloud solutions was conducted. It entailed visiting the various government institutions and interviewing the ICT personnel on the availability of implemented cloud solutions, offered services and their service providers. These questions were also included in the main questionnaire.

3.3 Sources of Data, Population and Sample size

There are many public institutions in Kenya. Most of these institutions are yet to adopt to cloud technologies. The target groups are those institutions that have embraced cloud computing and those that are IT enabled. After a preliminary study of government parastatals with cloud solutions was conducted, six (6) government parastatals were selected. Each of the institutions was to produce seven (7) ICT staff at least three (3) from senior or management position. The targeted population for the study include ICT managers and staff in ICT department, managers involved in policy making decisions on computing. The total population targeted was 42 respondents as depicted in the following diagram.

3.4 Data Collection

Collecting credible data is a tough task and it is worth remembering that one method of data collection is not inherently better than the other. Data collection consists of either primary or secondary data. The use of primary data cannot be over emphasized. However secondary data may also be collected to augment the primary data.

3.4.0 Data collection technique

To collect primary data the survey method of data collection has been selected. Surveys were conducted via questionnaires. The researcher used closed and open ended questions to obtain responses from the interviewee, who will be the primary data for the study. This format makes it easier to code, analyse and compare data. The questionnaire will use structured questions consisting of approximately 29 questions divided into five sections A, B, C, D, and E. Most of the question will be closed ended and respondents will be asked to tick the appropriate answer. Some questions however will require respondents to give opinions.

3.5 Data analysis

This is a process of observing patterns in the data asking questions of these patterns, constructing conjectures, confirming and refuting the conjectures. It presents mathematical interpretation of the relationship between independent and independent. After the data was been collected, on the respondents opinions on the service and deployment model implemented, security challenges and cloud data protection techniques, existing data security models the responses were summarized, edited, coded and allocated frequencies following the likert scale responses ratings to establish the mean, model variance, standard deviation and the correlation between variables. The descriptive statistical method was applied to measure and determine the relationship that exists among the collected data. Demographics were analysed using frequency graphs and the objectives were analyzed using mean and standard deviation to understand relationships between the variables of study.

Descriptive analysis using mean and mode were used to understand and interpret variables; also standard were used The data was analyzed and the research findings were presented using frequency tables, pie chart and bar graphs as appropriate.

Analysis tools used were Statistical package for social science (SPSS) and Excel to obtain percentages, tabulations, means and central tendencies.

CHAPTER 4

RESULTS AND DISCUSSIONS

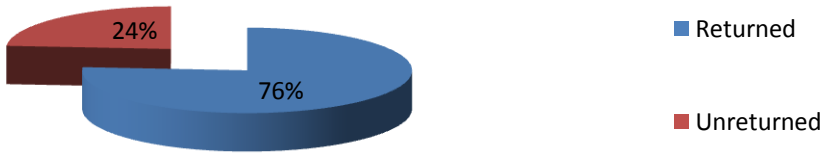
4.1 Introduction

This chapter presents a report on the interpretation of the findings of the study as set out in the research methodology. It focuses on a descriptive and quantitative analysis of the elements of the data security implementation model for cloud computing in government parastatals. The research data was gathered exclusively through questionnaires as the primary research instrument. The questionnaire was designed in line with the research objectives of the study. The research broad objective was to design a data security implementation model for cloud computing in government parastatals.

4.2 Response Rate

The survey targeted 42 respondents from six IT enabled government parastatals who may have implemented the cloud computing. The targeted respondents for the study were ICT managers, supervisors and employees aligned to cloud computing in the ICT department. 42 responses were expected, however only 32 responses were received while 10 respondents did not return filled questionnaires resulting to a 76% response rate. This response rate is considered good since according to Mugenda and Mugenda (2009) a response rate of 50% is adequate for analysis and reporting; a rate of 60% is good and a response rate of 70% and over is excellent.

Figure 4.1: Response Rate



As shown in the table 4.1 below a total of 42 responses were expected. It is only 32 responses that were received as 10 respondents did not return filled questionnaires despite several personal visits and phone calls to their institutions. The percentage response rate for the sampled government parastatals was as shown in the table below.

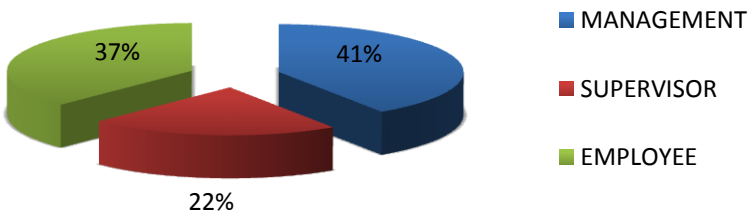
Table 4.1 Parastatals response details

	Questionnaires			%
Parastatals	Issued	Returned	Unreturned	Response rate
KPLC	7	6	1	86
KRA	7	5	2	71
PCK	7	4	3	57
KENET	7	4	3	57
ICTA	7	7	0	100
CAK	7	6	1	86
Totals	42	32	10	76

4.3 General information

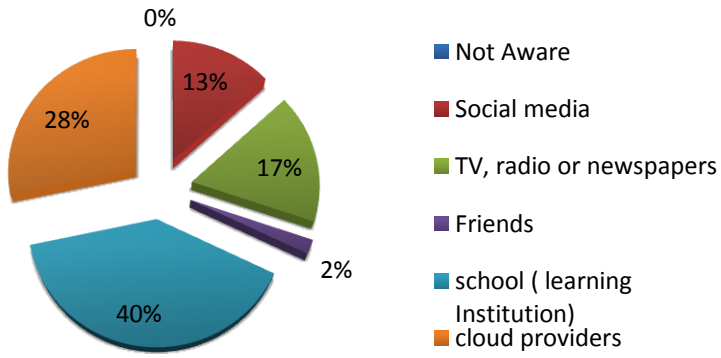
The study sought to find out the current position, the department of the respondents and where they learnt about cloud computing. According to the findings, 100% of the respondents belonged to ICT department 40% of the respondents were ICT directors, heads and managers, 38% of the respondents were supervisors and 22% of the respondents were employees.

Figure 4.2: Current position in the parastatals



The study sought to find out the level of understanding and the main source of the cloud information among the respondents. Out of the 32 respondents 40% learnt about cloud computing from learning institutions, 28% learnt about cloud computing from cloud providers, 17% learnt about cloud computing from TV, radio or newspapers, 13% learnt about cloud computing from social media, 2% learnt about cloud computing from friends of family and 0% are unaware.

Figure 4.3 Main source of cloud computing information



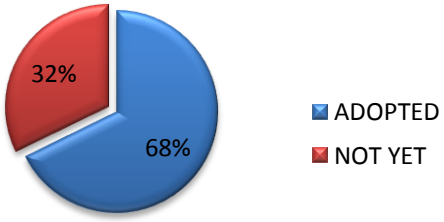
4.3.1 Analysis and discussion

The study shows that most of the respondents were either ICT heads, managers, directors or supervisors. This people are in a position to make and or advice on core decisions about the parastatal's ICT department such as those that involve migrating some applications to the cloud. It also shows that all respondents are informed about cloud computing from two or more sources. Most of them learnt about cloud computing from a learning institution, cloud providers, mass media and other sources. This helps the study in ensuring that the information given by the respondents is reliable.

4.4 Cloud computing adoption

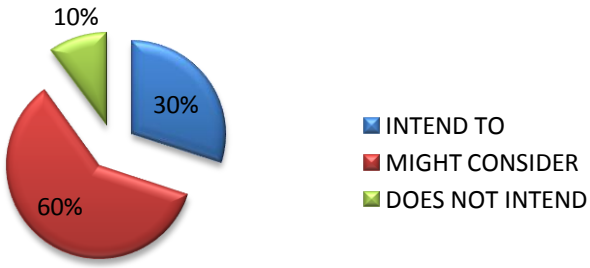
The study findings show that 68% of the sampled parastatals have adapted to cloud computing while 32% have not yet adopted to cloud computing. The figure 4.4 below shows cloud computing adoption findings in percentages.

Figure 4.4 Adoption to cloud computing



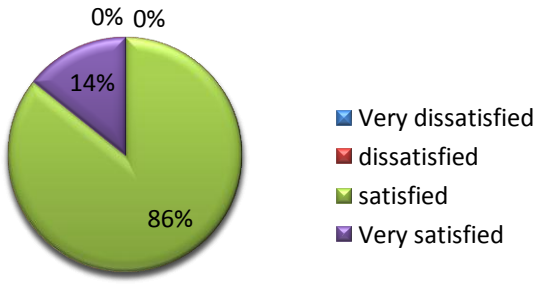
Out of those 32% that had not adopted to cloud computing the study sought to find out whether there was any intention to adopt to cloud computing technologies in the near future. The findings as shown in figure 4.5 below indicate that 30% intend to adapt to cloud computing, 60% might consider and 10% stated categorically that they will not adapt to cloud computing technologies. They pointed out that their institutions lacked capacity to venture into such a new technology and mainly they feared that cloud security standards and policies were not mature thus posing a high risk of moving to cloud.

Figure 4.5 Level of intention to adopt to cloud computing



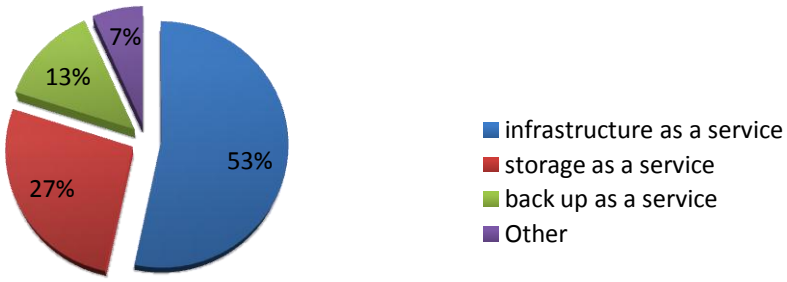
Out of the 68% that had adapted to the cloud computing the study sought to find out the level of satisfaction with the cloud technologies. As shown in figure 4.6 below 86% of those that have adopted to cloud computing are satisfied with cloud service while 14% very satisfied and none were dissatisfied.

Figure 4.6: Level of satisfaction with the cloud service



As depicted in the figure 4.7 below, the study established that more than one cloud service was in use in most parastatals. 53% of the respondents indicated that their parastatals were using the infrastructure as a service, IaaS entails virtualisation of hardware such as Virtual machine, storage, OS environment. According to the study IaaS has a lower risk of attack since the user has control over the security compared to other service models. 27% were using storage as a service, 13% were using back up as a service and 7% were using other cloud services. This means that 40% of the GPs are sensitive to their data and have provided for more storage space via cloud or a back up in case the main storage failed or compromised a backup has been provided off premise thus ensuring data safety.

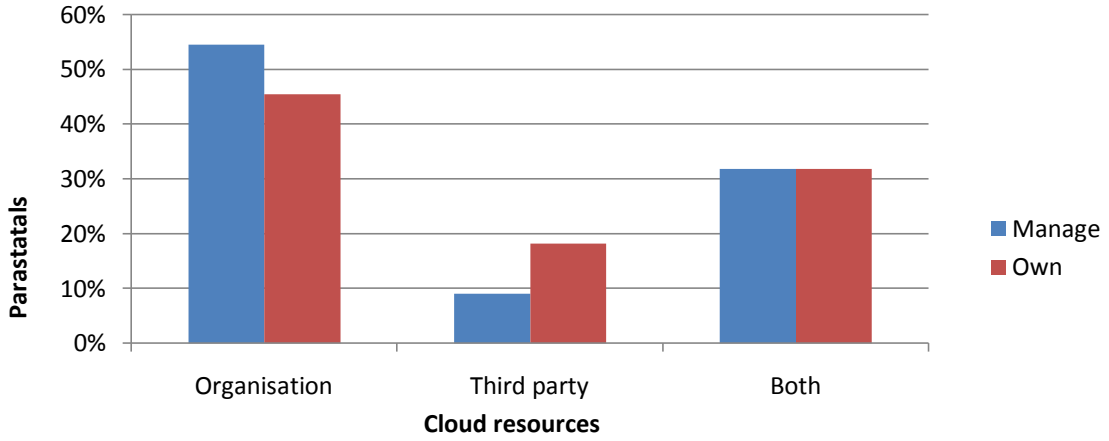
Figure 4.7: Cloud computing service currently in use in the parastatals



As depicted in figure 4.8 the study sought to establish the Management and ownership of cloud computing data and resources in the parastatals. 55% of cloud data and resources are managed by the organisation, 32% are shared where the organisations manage some cloud resources while third party

manages some resources and only 9% cloud data and resources are purely managed by a third party. The study also indicated that 45% of cloud data and resources are owned by the organisation, 32% is shared between the organisation and the third party while 18% of cloud data and resources are owned by the third party. (Bernice et al., 2011) Argue that data ownership is a question that should be discussed and clearly defined on the SLA before the client has deployed the services. This protects the clients from a data or vendor lock-in risk if he decides to change the CSP or engage another CSP for other services.

Figure 4.8 Cloud data resource management and ownership



96% of the respondents agreed that their organisations need to migrate some of their services to the cloud. They gave examples of such services as Email and exchange services but not services such as customer information services which were too sensitive in their opinion. Most of the GPs may like to migrate their systems to cloud due to numerous benefits. Cloud computing is a low cost viable option for users, building a highly available cloud infrastructure is not necessarily costly or laborious. Furthermore GPs can use their existing infrastructure which is likely to be under used at present thus increase in operational efficiency and productivity. 4% disagreed of their organisation migrating to the cloud. The following figure 4.9 illustrates the likelihood of organisations migrating some of their services to the cloud.

Figure 4.9: Likelihood of the organisation to migrate some of its services to the cloud

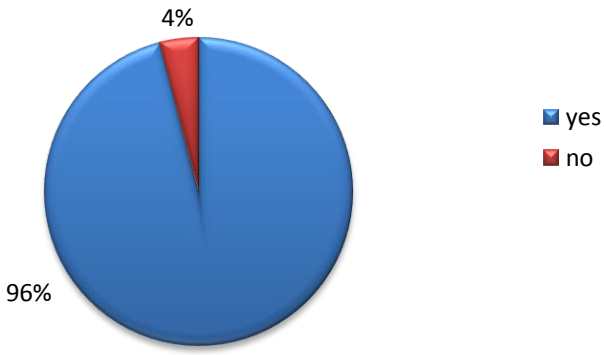
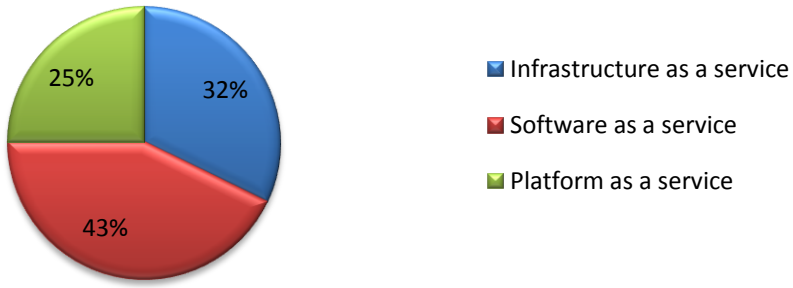


Figure 4.10 below outlines the respondent's opinion on which cloud services they would advise their organisations to deploy. 43% preferred software as a service, 32% preferred infrastructure as a service and 25% preferred platform as a service.

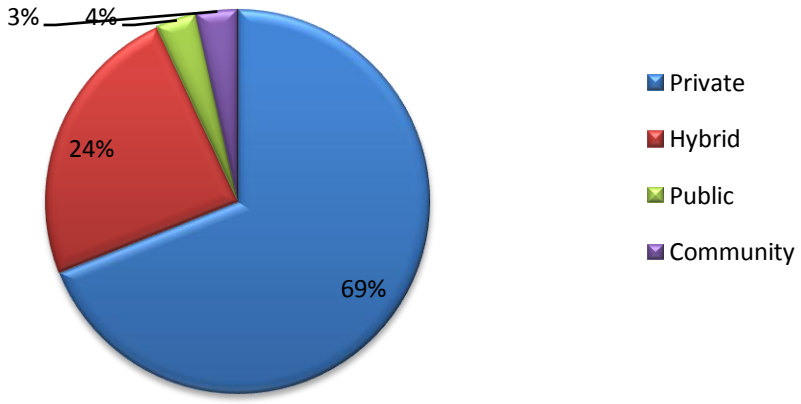
Acquiring software or going through the rigorous process of developing software is tedious and expensive. Many organisations may prefer acquiring software from a provider who will develop, maintain and ensure its security while the organisation will only pay for what they will have used at a low cost, in addition most of the key GPs have an existing ICT infrastructure thus most parastatals preferred SaaS. Iaas is the second most preferred cloud service in this study because it involves the virtualisation of hardware such as the server, database or storage and OS. The provider controls and manages this layer ensuring its security while the user controls the application, user interaction and data while ensuring its security. It provides the user with some level of control over their applications and data lowering the risk of unauthorised access from the provider's side. There are not many GPs in the development and deployment of applications though some many develop systems for organisational functions and hence only 25% preferred PaaS for their organisation.

Figure 4.10: Cloud services preference for deployment in the organisation



To understand the organisations under study figure 4.11 illustrates the responses on the cloud models deployed in the organisations currently. 69% had deployed private cloud, 24% had deployed hybrid cloud model, 4% had deployed public model and 3% had deployed community model. 69% of the GPs deployed private cloud mainly because it is perceived to be easier to align with security, compliance and regulatory requirements and gives the organisation control over deployment and use. It is regarded as the more secure that other models since only the organisation and designated stakeholders have access to operate on a specific private cloud. In addition, some GPs in the past invested heavily in ICT and have the capacity to man a private cloud and even offer some of their vast resources to other cloud users (E.g. KPLC has offered some of its infrastructure to safaricom) especially in the government or even private sector. Some of the GPs deployed a hybrid model which entails combining the private cloud with one or more external cloud services. Security of the hybrid model is relatively lower as compared to private model since access and control is divided between the client and the provider thus exposed to some level of security risk. Only 3% preferred public model, this may be due to its high vulnerability risk and the fact that the user lack control over the resources.

Figure 4.11: Cloud models deployed



4.4.4 Analysis and discussion

Most parastatals have adopted to cloud computing however are uncomfortable with the idea of storing their data and applications on systems they do not control, thus the highest percentage of the parastatals have deployed private and hybrid cloud. Migrating workloads to a shared infrastructure increases the potential for unauthorised access and exposure. Some of these parastatals that have not adapted to the cloud disclosed that they intend to migrate some of the services which are undergoing testing to the cloud. They were exploring different models for which they would deploy. Iaas and SaaS are the most preferred services that most parastatals have deployed followed by Paas. Management and ownership of data and resources is an important aspect in cloud computing. Cloud computing raises questions of ownership and accountability within ICT groups across the organization and extending to service providers and other vendors. In this study most parastatals preferred to manage and own their cloud resources, followed by both (the parastatal and the cloud service provider) parties managing cloud data and resources and only a few parastatals preferred their cloud resources to be managed by the third party.

4.5 Cloud computing security challenges and threats affecting cloud data and resources

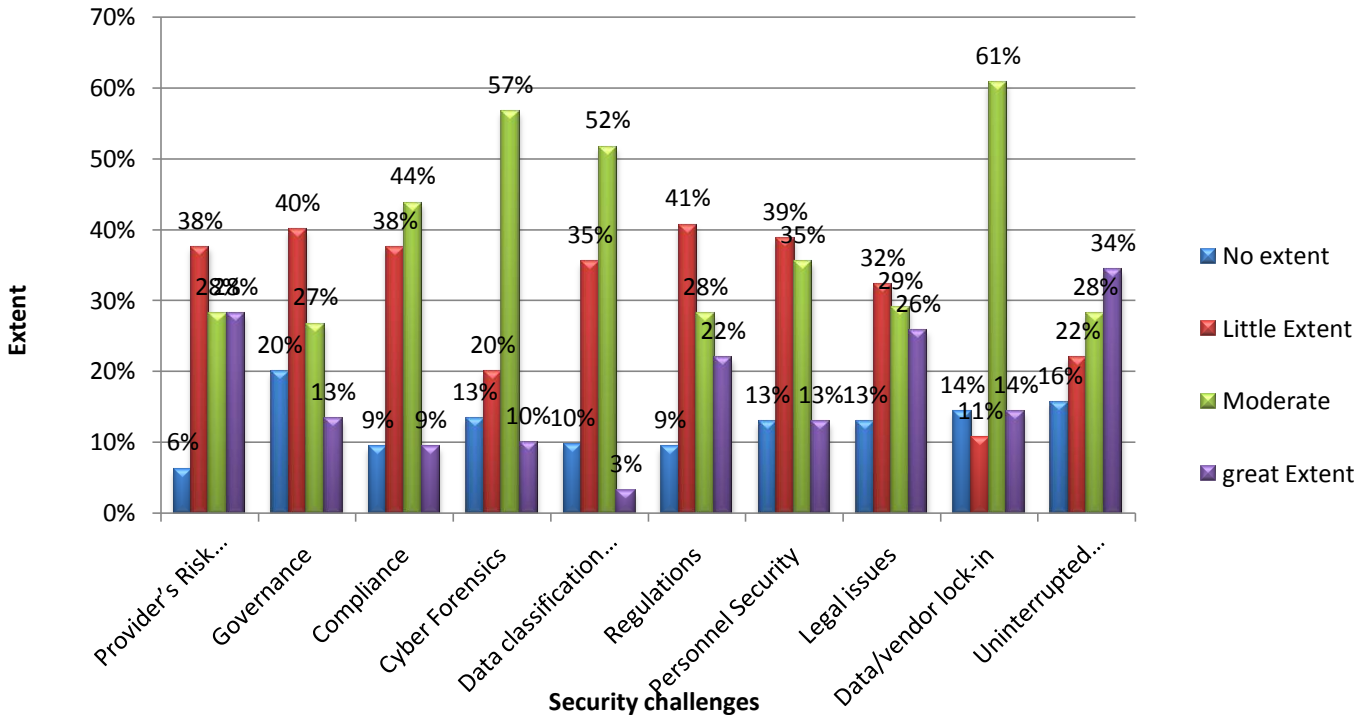
In this section the study establishes the extent to which different security challenges and threats affect the security of cloud data and resources. 93.7% of the respondent agreed that security is one of the major challenges hindering fast uptake of cloud technologies not only in government parastatals but also in the private sector while 6.3% were indifferent. Cloud computing challenges were classified into two: firstly, legal, policy and organisational challenges and secondly technical and security challenges. The data in

figure 4.12 and 4.13 below are compressed into four levels namely no extent, little extent, moderate extent and great extent. This has been prompted by the fact that the challenges and threats affect the organisations cloud data and resources to a certain extent or no extent. The findings in percentage of the four levels are presented in form of a bar chart and a column chart respectively.

4.5.1 Legal, Policy and management challenges affecting security of cloud data and resources

Cloud computing presents a number of management challenges. Each type of cloud presents its own set of management challenges. The study sought to find out the degree to which these challenges affect their respective organisations cloud data and resources. 97% of the respondents expressed different opinions on each challenge while 3% of the respondents did not have adequate information on cloud security.

Figure 4.12: Degree to which legal, policy and organisational challenges affect the security of cloud computing data and resources and.



From the chart many parastatals have been affected to a certain extent as follows. Providers risk profile unknown issue affected 38% of the GPs slightly, 28% moderately, 28% greatly and 6% were not affected. From the study it is evident that 94% of the GPs. The respondents agreed that there were pertinent information about their CSP that was overlooked such as internal security procedures compliance,

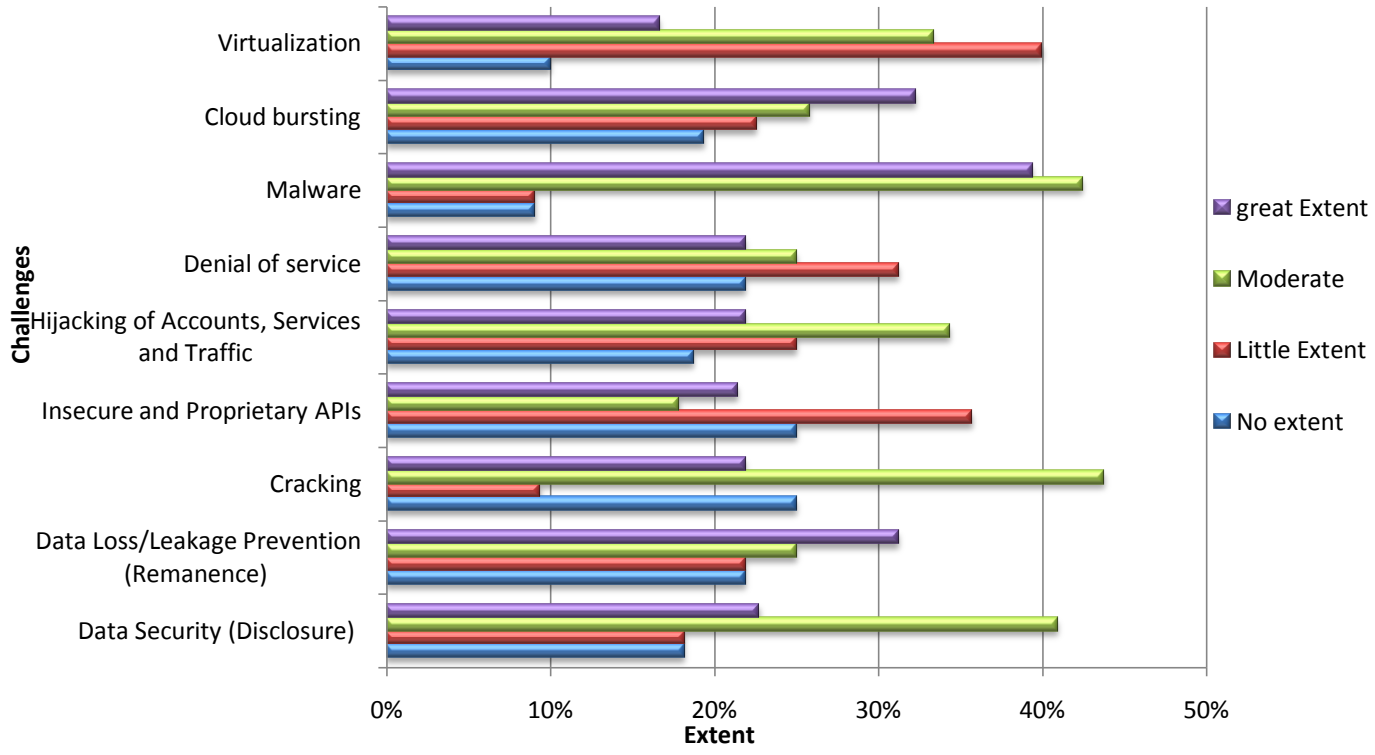
auditing, logging, hardening, data and related logs storage and access. Most GPs have issues surrounding providers profile when adopting a cloud service. Governance affected 40% of the parastatals slightly, 27% moderately, 13% greatly affected and 20% were not affected. 80% of the GPs had been affected in one way or another by governance issues. Most respondents that there were no standard cloud governance frameworks that can coordinate and direct their overall approach to the management of the service and information within it. Most of them use the existing ICT governance frameworks like COBIT. However cloud services and data management is very different from the traditional management of data. Compliance issues have moderately and slightly affected 44% and 38%respectively, 9% were greatly affected and 9% were not affected. Compliance issues cut across all organisations. They are immediately initiated by cloud services. These can rather be complex owing to the fact that multiple territories with different jurisdictions may be involved. Cyber forensics affected 57% of the GPs moderately, 20% slightly, 10% were not affected and 10% were greatly affected. Since cloud computing is a young technology, when there is security bleach establishing forensic capabilities for cloud organizations is difficult without handling several enormous challenges. Cloud computing raises some unique law enforcement concerns regarding the location of potential digital evidence, its preservation, and its subsequent forensic analysis. There are also potential forensic issues when the customer or user enter or exits a cloud application. Items subject to forensic analysis, such as registry entries, temporary files, and other artifacts (which are stored in the virtual environment) are lost, making malicious activity difficult to substantiate and thus 90% of GPs have issues concerning cyber forensics. Data classification and labelling affected 34% slightly, 53%and 9% were moderately and greatly affected respectively and 4% were not affected at all. The largest percentage of the GPs were either slightly or moderately affected. Classification of data based on its level of sensitivity and the impact to an organisation should be detailed should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. This is important especially for hybrid cloud where in case of a cloud burst sensitive data may proliferate to public domain bring about security bleach. Regulations issues affected 41% slightly, 28% moderately affected, 22% were greatly affected and 9% were not affected. Personnel security affected 39% slightly, 35% moderately, 13% greatly and 13% were not affected. This is one of the key concerns in the cloud adoption as 87% of the respondents agree. CSP staff should undertake personnel security screening and security education, they should be trustworthy and they should be checked against a recognised personnel security standard. Legal issues affected 26% greatly 29% moderately, 32% were affected slightly and 13% were not affected. Vendor/ data lock in affected 14% of the GPs greatly, 61% moderately, 11% were slightly affected and 14% were not affected. The larger percentage of the respondents has been affected and only 14% were not affected. When adopting to cloud it's important to choose a provider that would allow the

user to move easily to another provider when needed. Uninterrupted availability affected 34% greatly, 28% moderately, 22% slightly and 16% were not affected. Cloud services and applications are expected to be always available when needed. However this is not always the case especially in bad weather with a lot of lightning power outages are common. CSP use UPS which can sometimes fail.

4.5.2: Technical and security challenges and threats affecting cloud data and resources.

These are security concerns that occur if sensitive data lands on public cloud servers, budget concerns around overuse of storage or bandwidth and proliferation of mismanaged images. Managing the information flow in a hybrid cloud environment is also a significant challenge. On-premises clouds must share information with applications hosted off-premises by public cloud providers and this information may change constantly

Figure 4.13: Degree of technical and security challenges affecting cloud data and resources.



The following summaries were observed from the column graph

Virtualization affected 17% of the GPs greatly, 33% moderately, 40% slightly and 10% were not affected. In virtualised environments physical servers run multiple virtual machines on top of the hypervisors. An attacker can exploit a hypervisor remotely using vulnerability present in the hypervisor itself. In addition a virtual machine can escape from the virtualised sandbox environment and gain access to the hypervisor and consequently all virtual machines running it. From the results of the study 90% of the GPs have been affected meaning that there exists a challenge in the virtualisation and thus mitigation methods within the GPs need to be improved. Cloud bursting is used when an application running in a private cloud or data center experiences a spike in demand for computing capacity that cannot be met with existing resources. An application "bursts" into a public cloud to access extra compute resources on an as-needed basis, and the organization only pays for the resources that are used.

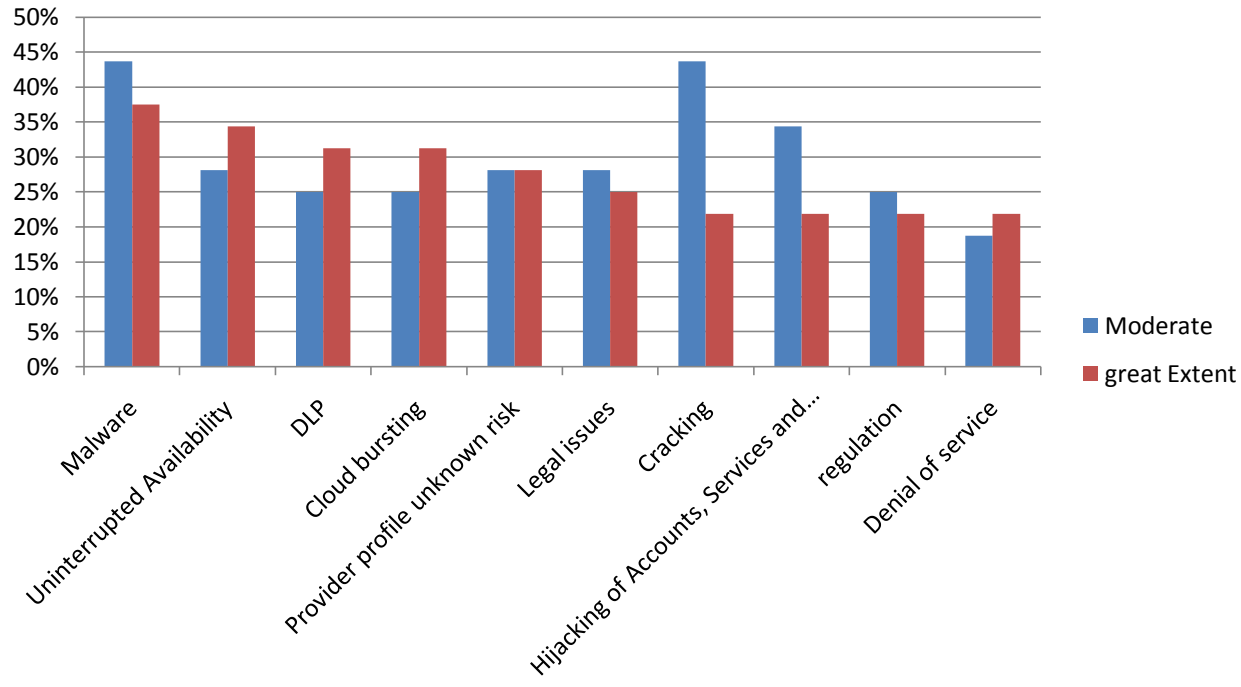
Cloud bursting clearly is a major challenge for many GPs. It affected 32% greatly, 26% moderately, 23% slightly and 19% were not affected. Cloud bursting complex infrastructure can be challenging to manage There are three main challenges facing organisations when utilising cloud bursting. They include configuring and managing cloud bursting, latency and security. There is need to ensure that the cloud provider offers the necessary compliance for your requirements within the environments. It's essential so that sensitive data is not placed at risk when bursting into a public environment because you the business is ultimately responsible for your data and for ensuring that it remains secure. When using cloud bursting its essential to establish a means to secure the communication path between the clouds. When data bursts from a secure private cloud into a public cloud this concern is exacerbated. It's advisable to set up an encrypted channel between the two cloud environments to prevent violation of the data through interception. It is advised to use SSL. Hijacking of accounts services and traffic affected 22% greatly, 34% moderately, 25% slightly and 19% were not affected. The study shows that hijacking of accounts services and traffic is prevalent since 81% of GPs studied, their accounts were hijacked and only 19% were not hijacked. An attacker gaining access to an account can manipulate and change the data and therefore make the data untrustworthy or turning off a web server making a website inaccessible. Most often it's only a case of a password required to access an account. A two-factor authentication is therefore preferred.

Malware affected 39% greatly, 42%moderately, 9% slightly and 9% were not affected. Malware is significantly affecting the security of the GPs. In fact, it has been ranked as the one of the key challenges that is affecting GPs at a great extent. Denial of service affected 22% greatly, 25% moderately, 31% slightly and 22% were not affected. From the study 82% were affected three or more times. In addition, 78% of the GPs were inaccessible resulting to a DoS attack at least twice and 47% were attacked for more

than 4 times. There is need to improve security measure such as a stronger antimalware and stronger authentication techniques. Insecure and proprietary APIs greatly affected 21% of the GPs, 18% moderately affected, 21% slightly affected and 25% were not affected. APIs are accessible from anywhere on the internet; malicious attackers can use them to compromise the confidentiality and integrity of customers. Only 39% of the GPs have been affected by the insecure APIs more than three times and 18% at least twice. These results show that the GPs have not been so affected but measures should be taken in order to decrease these effects to a minimum level. Cracking affected 22% of the GPs greatly, 44% moderately, 9% slightly and 25% were not affected.

Data loss/leakage prevention affected 31% greatly, 25% moderately, 22% slightly and 22% were not affected. Data loss entails losing data due to hard drive failure or CSP accidentally deleting clients' data. These results show that some data loss has happened in the GPs at least twice or more for 78% of the GPs. There is need for better back up strategies to prevent data loss. Data security (disclosure) affected 23% of the GPs greatly, 41% moderately, 18% slightly and 18% were not affected. Data disclosure may occur if VM is able to access data from another VM on the same physical host. Data bleach is a common security issue and it is evident that the GPs had had a great deal of data disclosure since 82% of the GPs has had a data bleach thus more security measures are need to ensure data is safe at all costs.

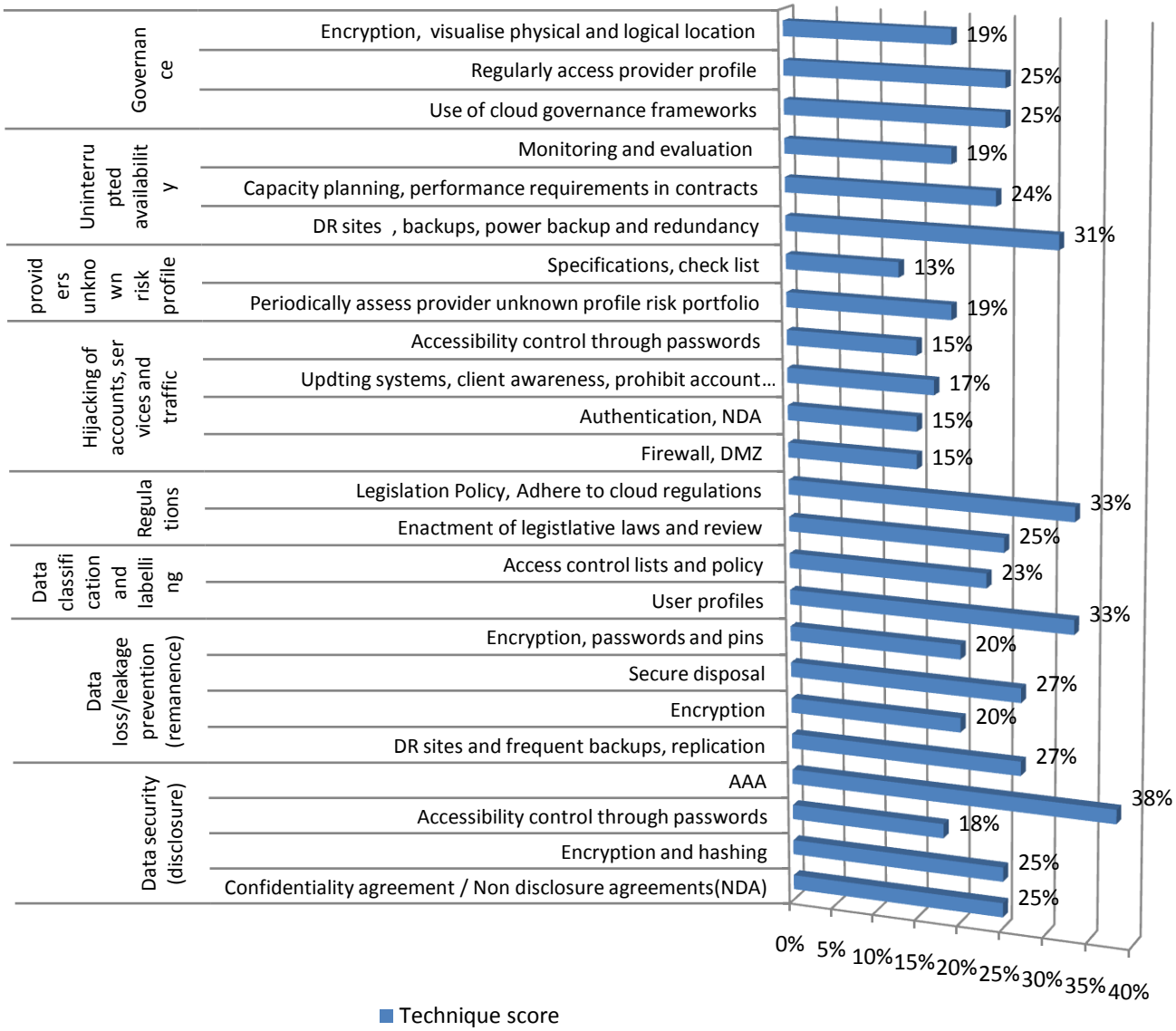
Figure 4.13.1 Key Cloud Computing challenges in GPs



4.5. Discussion.

All the challenges highlighted in this section have affected the GPs to a certain extent. The figure 4.13.1 shows the first ten(10) challenges that have greatly affected the GPS. This finding resulted from the statistical ranking where the challenges that affected the GPs five and above times(i.e. great extent) were ranked from the highest to the lowest and then those that were moderately affected(i.e. Three to four times) were ranked next. These challenges and/or threats are listed as follows from the first(1^{st}) to the tenth(10^{th}) : they include 1) Malware, 2)Uninterrupted availability, 3) Data loss(remanence), 4)Cloud bursting, 5) Provider profile unknown risk 6)Legal issues 7)Cracking, 8) Hijacking of accounts, services and traffic 9) Regulations and finally 10) Denial of service.

Figure 4.13.2 Techniques to mitigate organisational challenges affecting security of cloud data and resources



4.6.1 Techniques to mitigate organisational challenges affecting security of cloud data and resources

As depicted in the figure 4.13.2 above the respondents listed various techniques that may be used to mitigate against the various challenges investigated earlier. Out of the techniques listed for each challenge an average score was found and all techniques above the average score were given preference. The following table displays the most preferred technique to mitigate cloud security challenges.

Table 4.13.2 below illustrates threat mitigation techniques for the first ten threats that were found having greatly affected the GPs.

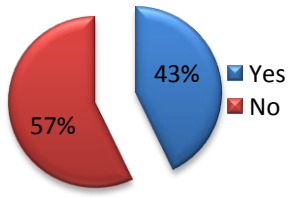
Table 4.13.2 Security challenges mitigation techniques

Threats	Mitigating techniques
Cracking	Tunnelling, Hardened infrastructure platform and applications Authentication, Firewall, DMZ
Hijacking of Accounts, Services and Traffic	Timed out sessions, session management Firewall, DMZ, Access logs, Two- factor authentication, NDA Updating systems, client awareness, prohibit account credentials sharing Accessibility control through passwords
Denial of service	Firewall, Redundancy, back up, QoS agreements Capacity planning, up-to date antivirus Standardised API, avoid proprietary API
Malware	Sandboxing, application and file visibility Antimalware, up-to-date antivirus, firewall, Tunnelling string authentication,
Cloud Bursting	Virtualisation, Firewall Security and regulatory compliance requirements Ensuring adequate capacity, Scaling capacity to handle spikes
Provider's risk profile unknown	Periodically assess provider unknown profile risk portfolio Specifications, check list, undertake due diligence and evaluate cloud service provider, Employee background check , Pen testing and auditing
Uninterrupted availability	DR sites , backups, power backup and redundancy Capacity planning, performance requirements in contracts
Compliance	Access and audit Logs, Regularly access provider profile
Regulations	Regular review of ICT and internal policy Enactment of legislative laws and review Legislation Policy, Adhere to cloud regulations
Data loss/leakage (remanence)	DR sites and frequent backups, replication Secure disposal, Encryption, passwords and pins
Legal issues	Clear contractual agreement and proper policy, legislation to enact cloud security laws and proper policy

4.6 CLOUD DATA SECURITY

In this section the study examines the need, availability characteristics of the cloud frameworks in the GPs and the role of the cloud service provider in the implementation of the cloud resources. The study sought information on the existence of cloud governance frameworks followed in the implementation of the cloud in the GPs. 97% response rate was recorded. The findings indicate that 43% had a framework while 57% didn't have. Most organisations used traditional

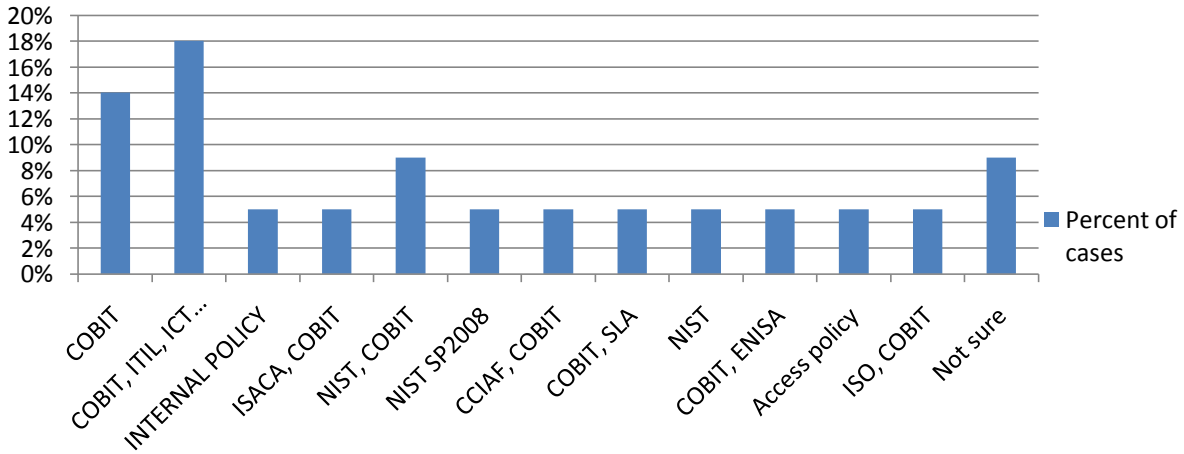
Figure 4.14 Existence of a cloud governance policy



4.6.1Cloud governance framework

The study sought to find out the governance frameworks that the GPs or their CSP were using to coordinate, manage their cloud services. Most of them are traditional ICT governance frameworks such as COBIT, ITIL, and ISACA. The highest percentage was 18% are using a combination of COBIT, ITIL, ICT policy, 14% purely used COBIT, 9% used a combination of NIST guidelines and COBIT and 9 cases of 5% used either internal policy, ISACA and COBIT, NIST and COBIT, CCIAF and COBIT, NIST, ENISA and COBIT, ISO and COBIT and 9% were not sure which framework they were using. This information is depicted in the figure 4.15 below.

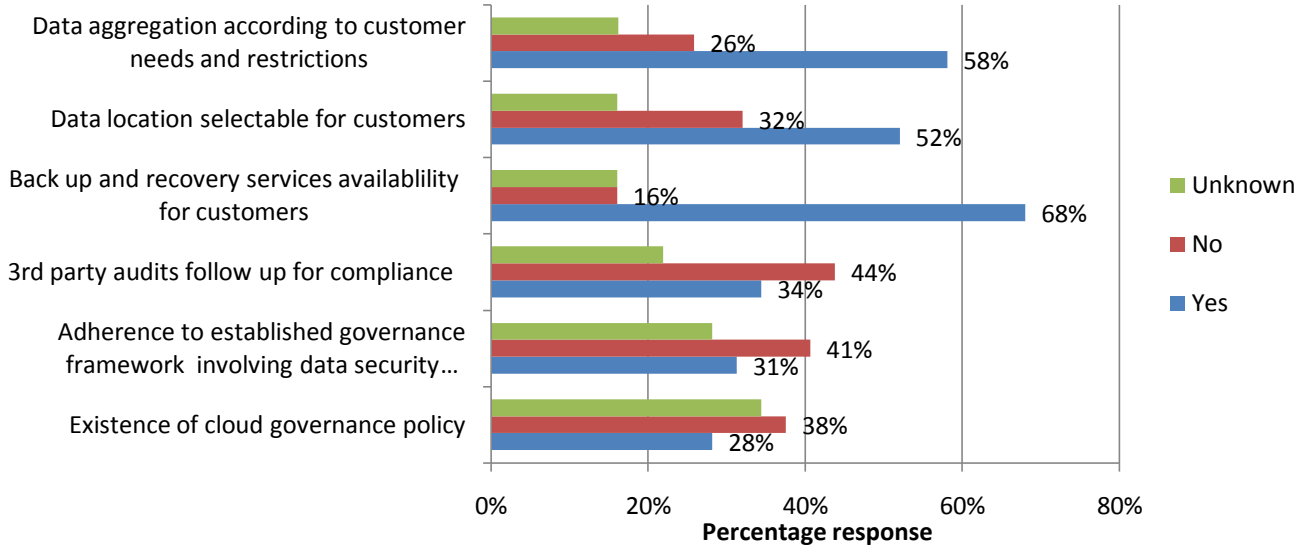
Figure 4.15 Cloud governance frameworks in use in the GPs



4.6.2 Cloud governance policy existence, adherence, third party audit, back – up, location selection and data aggregation.

The study sought to find out the existence of cloud governance policy in the GPs, 28% had the policy, 38% did not have the policy in their organisation and 34% were not sure whether there was a cloud governance in their organisation or not. This result shows that 72% of the GPs do not have a documented ICT policy which contains a cloud adoption policy in the event there was a need to use some cloud services. There are governance frameworks available, the study sought to find out whether the GPs adhered to some of these frameworks in their data security controls. 31% adhered to some data security controls with some framework, 41% do not adhere to any framework and 28% were not aware. This shows that only a third of the interviewed GPs have a framework that they follow, and the rest don't have or are not aware. This brings the need for the organisation to analysis a documented cloud framework that they can adopt and also conduct user training to their staff so that they have adequate information on the cloud dealings especially security. 34% had third party audits follow ups, 44% did not have and 22% were not aware whether there were any audit follow up. Third party audit helps to ensure that the CSP is following laid down agreements, procedures, policies, contracts, standards, laws. More than half of the GPs do not have third party checks on the CSP and thus may results to the high number of concerns among the GPs. 68% had backup and recovery services in place, 16% did not have backup and recovery services and 16% were no aware of the availability of the service or not. Backup and recovery services have been implemented by more than two thirds of the GPs. The study also sought to know whether the customer had the ability to select their data location or not. This is important because different organisations policy stipulate where the organisations data is located. CSPs may store organisations data locally or even abroad. Data location greatly affect cyber laws, jurisdiction that the CSP would operate in. 52% were able to select their data location, 32% could not select their data location and 16% didn't know whether data location was selectable to them or not. There has been a concern on the commingling of customer data especially in public cloud. The study sought to find out whether CSP provided data aggregation for the customers data according to customer needs and restrictions. 58% agreed that their CSP provided for data aggregation, 26% had no data aggregation provision and 16% did not know whether that provision was applied by their CSPs.

Figure 4.15 Cloud data governance, control, organisation and security



4.6.3 Identifying a suitable cloud service provider

The key reason for this research area is find out how cloud users can identify a suitable cloud provider, evaluate the service offering and understand how CSP handle service security and clients' data security. The respondents listed a number of ways a cloud user could identify a suitable service provider. They include: a) Using a cloud service need specification b) CSP Customer feedback, c) Service provider profile d) Vetting using provided checklist such as access privileges, data recovery, business continuity, monitoring and reporting d) Billing capable team e) Adoption of the organisational Procurement policy f) Vetting of service providers using a laid down criteria and g) Using the need assessment report will help in identifying a suitable Service provider.

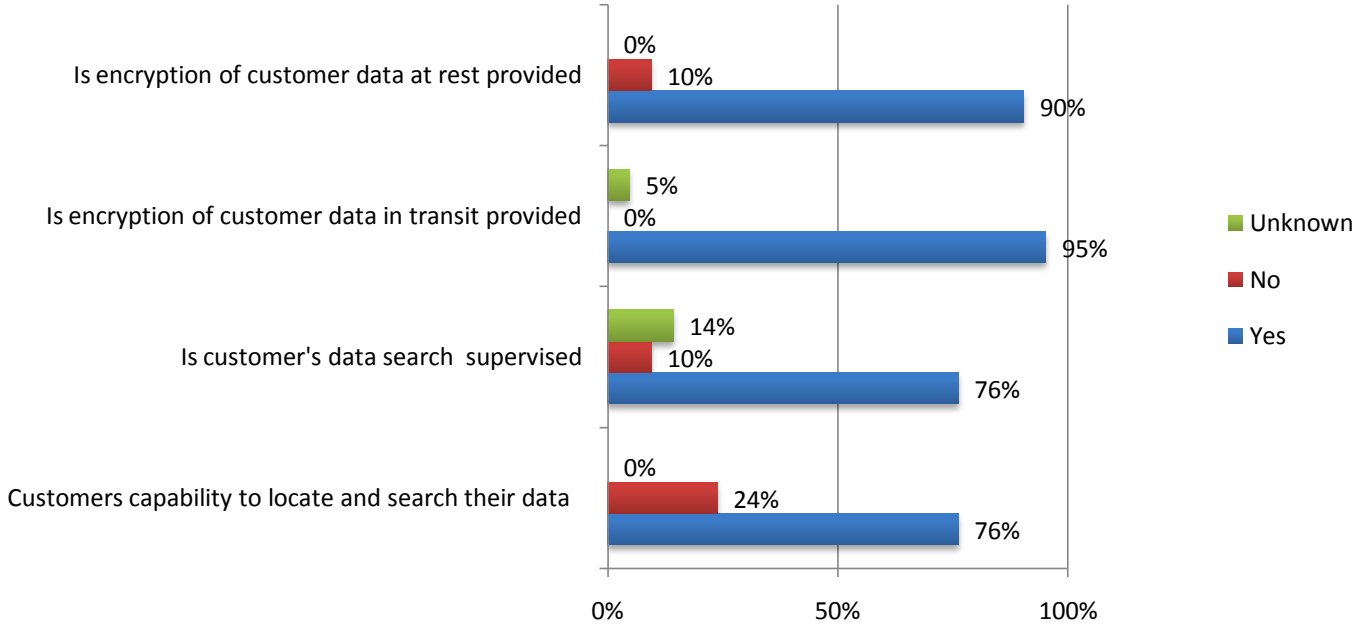
4.6.4 Evaluating the cloud service provider

After identifying the suitable CSP it was found paramount that an evaluation be conducted to ascertain whether the CSP meets the criteria. The respondents listed a number of ways they use and a cloud user may use to evaluate the CSP. They include a) Tendering and evaluation process, b) Portfolio, c) Customer audit d) Procurement processes and inspection e) Regulatory compliance f) Check list within ICT policy, g) Inspection of the CSP infrastructure and h) Analysing the provisions of the SLA and the QoS contract.

4.6.5 CSP data security

The study sought information on how the cloud user would be assured that once the data is migrated will remain safe. The following measures were listed. The cloud user was expected to verify and validate a) Providers assurance control claims, b) Migration and integration experience, c) Cost for service, d) CSP Internal policy provisions e) Availability of security resources, f) Service provider checklist e.g. regulatory compliance, service history, billing capabilities, g) Continuous improvement (ISO) provisions, h) Service level Agreements and contracts and i) Adherence to cloud security standards, frameworks and policies.

Figure 4.16 Cloud data search, supervision and encryption



In this section the study sought to identify security measures applied to data at rest and in transit, supervision of data search and customers capability to locate and search their data. It is evident that the GPs guard their data very well because 90% and 95% provided encryption on data at rest and in transit respectively. Since this organisation carry Government data which is very sensitive thus the GPs have invested a lot to ensure data is safe. 76% indicated that they were capable of locating and searching and they were supervised though 14% didn't know whether or not they were supervised, 10% were not supervised and 24% were not able to locate or search their data. Most of the data in the government is classified as sensitive and thus over 90% is encrypted for safety purposes, while some data is open for

public domain and other for organisational purposes. Thus 76% could locate data but these searches are monitored and only a small percentage of 10% is not monitored.

4.8 Data life cycle and security measures applied in each stage

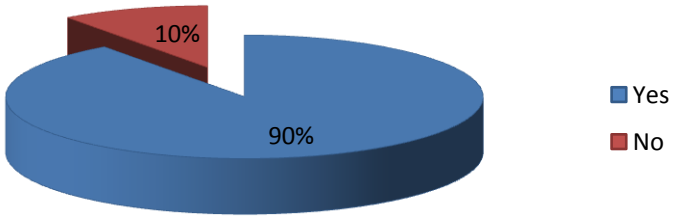
Every datum in any organisation goes through stages of importance to unimportance. (Mircea, 2012) Indicated that each stage of data life cycle security is key to ensuring an organisations data is secure. The study sought to identify security measures that can be applied to each stage of the data life cycle. The following are the views of the respondents. 1) Creation stage : User profiling, proper content design access, validation measures, structured data gathering, authentication of identities, Type checking, access control, Secure by design, User access rights management, tagging, classification levels, Encryption, quality assurance and User IDs 2) Sharing stage: Public folders encryption and passwords, Digital certificates , Sensitivity levels (profile / account control), use Secure Socket Layers (SSL) and transport layer security (TSL) protocols, audit trails encryption - digital signature, content encryption, application security, access controls, content monitoring and protection, access rights, and Designated data leakage prevention (DLP). 3) Maintain stage: Policy guidelines, authorisation, senior personnel, logs, access control lists, passwords and change triggers, data encryption, hardening of server, content discovery, audit trails, Log records, recovery plans, Asset management, data controls, user profiles and logical controls. 4) Storage stage: Tapes authorised by DBA, rights management, media and environmental controls, Backup, DR and updates passwords, encryption, logical controls access controls and log files. 5) Usage stage: Policy access in place authorised senior personnel, logs, ACLs, password, authorisation policies, physical and logical controls, recovery plans, access monitoring, enforcement, authentication, privilege levels, monitoring, user rights management and data labelling and backups. 6) Destroy stage: Policy to guide in place, legal rights, disposal regulations, secure deletion archiving and tape disposals with encryption, cleaning and recovery procedures, overwriting and most data is retained.

4.9 Cloud data security implementation model

4.9.1 Cloud data security implementation model (CDSM) need analysis

In this section the study sought to establish whether the GPs needed to adapt a CDSM. A 94% response rate was recorded where as illustrated in figure 4.16 below. The findings indicate that 90% agreed that there was a need for cloud data security implementation model and 10% indicated that the systems they had were sufficient for their operations. This result shows that there is dire need for cloud governance framework thus the need to adopt cloud data security implementation model (CSDM) is very high and it would be of benefit to the GPs.

Figure 4.17 need to adopt to a cloud data security implementation model



4.9.2 Challenges and security bleaches experienced in the GPs

In this section the study sought information about the challenges the GPs have been experiencing and security bleaches experienced in the past in the GPs. 91% responses were received for challenges expected to be solved by the CDSM as illustrated in table 4.8 and 86% responses were received for security bleaches experienced in the past for the GPs as illustrated in table 4.9.

Figure 4.13.2 Challenges and security bleaches experienced in the GPs

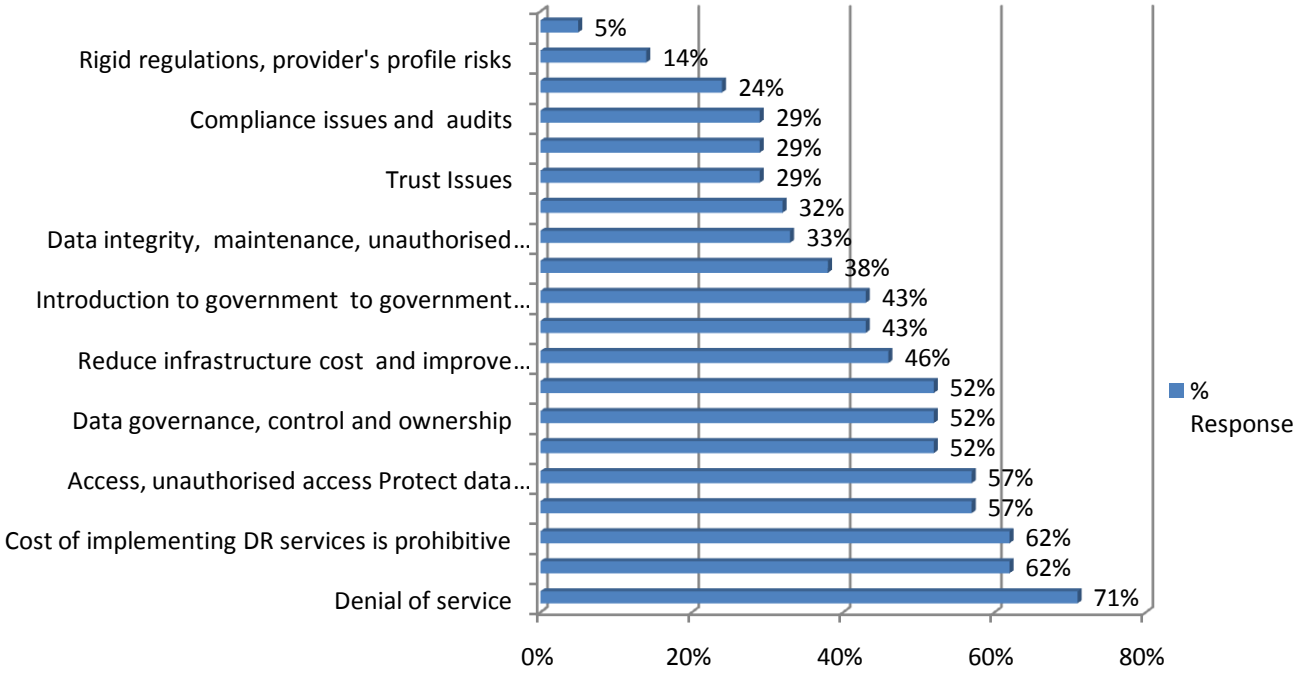
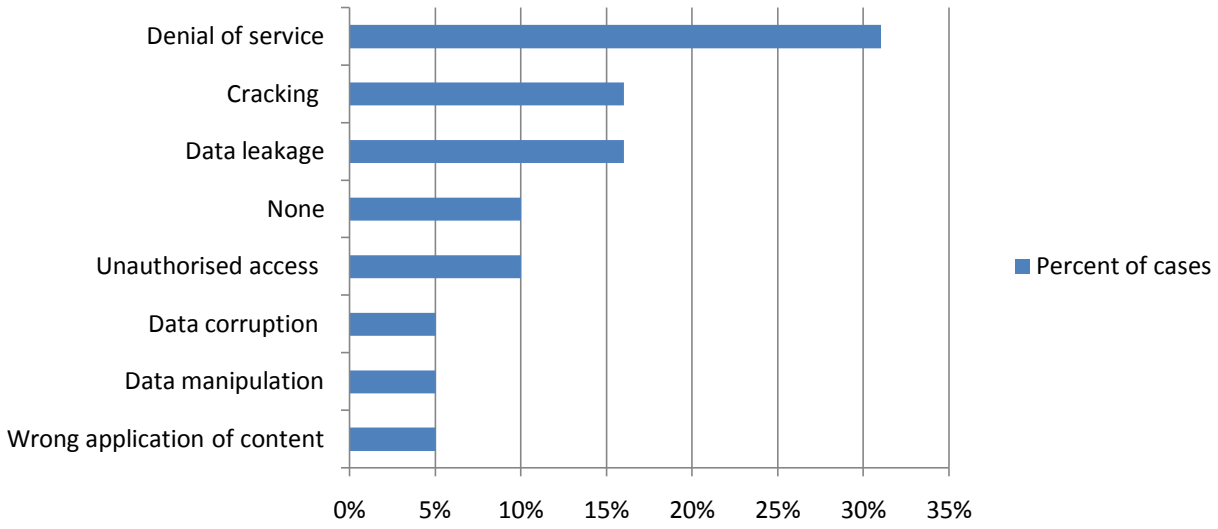


Table 4.8 illustrates a collection of the responses made by individual respondents indicating the challenges the GPs were facing and expected that the cloud data security implementation model (CDSM) would solve. Different respondents listed a number of challenges they were experiencing thus similar challenges would count in different respondents list. The views are ranked according the highest response

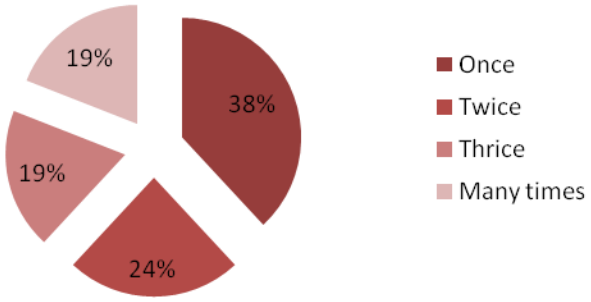
score to the lowest. The CDSM is expected to solve these challenges and most of these challenges are addressed at some point in the stages of the CDSM.

Figure 4.7.4 Security bleaches experienced in the past in the GPs



In table 4.9 the respondents indicated the security bleaches they had experienced before and the extent to which the bleach had affected them in a scale of 1 to 10 as illustrated in figure 4.13. 5% were affected by data corruption, data manipulation and wrong application of content. 16% were affected by cracking and data leakage each, unauthorised access affected 10%, denial of service affected 32% forming the highest percentage. 10% did not respond. This means that DoS is the most prevalent security bleach experienced within GPs followed by data leakage and cracking. GPs should improve or harden their security measures.

Figure 4.18 Rate of past security breaches in the GPs

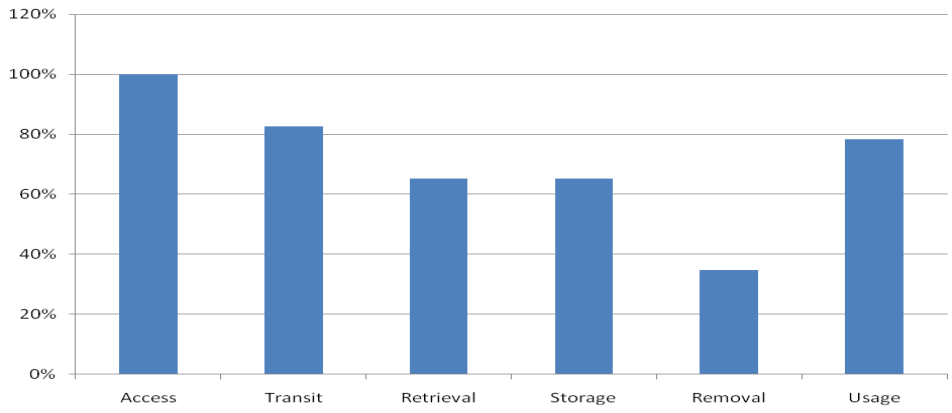


The findings indicated 97% response rate, the figure 4.13 above show 38% of the organisations had had a security breach at least once, 24% had been affected twice, 19% had been affected thrice and 19% had had security breaches more than three times. This result proves that security is still a major challenge among government parastatals thus the more reason they should adopt to the CSDM.

4.9.3 Areas the CDSM model is expected to cover in the GPs

The study sought from the respondents the areas the CDSM should cover. Six options were given where they would select one or more options. 97% response rate was recorded. The findings indicated that access with 100% was preferred by all organisations, transit with 83%, retrieval and storage were preferred with both 65%; removal and usage were preferred 38% and 78% respectively. This result show that access, transit, usage, storage, retrieval and removal, all arranged on the basis of highest to lowest percentage response need to be included into the CSDM since they all have received an average percentage score of 72% which is above average score.

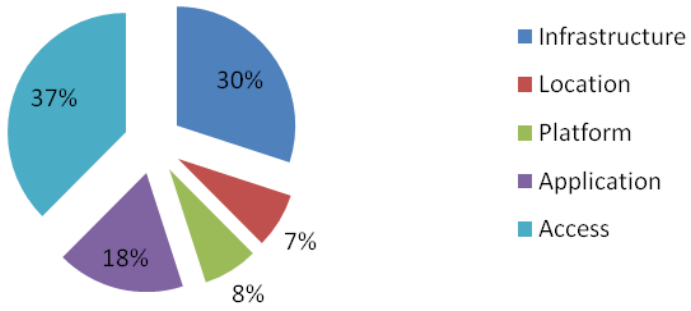
Figure 4.20 Areas the CDSM model is expected to cover



4.9.4 Cloud level or layer considered most vulnerable

The study sought information on the most vulnerable cloud level or layer. The figure 4.18 below indicates that access layer in the most vulnerable with 37%, infrastructure with 30%, application with 18%, platform with 8% and the least vulnerable cloud level is the location with 7%. This result show that access level/layer of the cloud is the most vulnerable and GPs should put more emphasis on securing this layer amongst other layers since they are also vulnerable to some extent.

Figure 4.21 Most vulnerable cloud level



Chapter 5

Proposed Framework and Discussions

5.1 Introduction

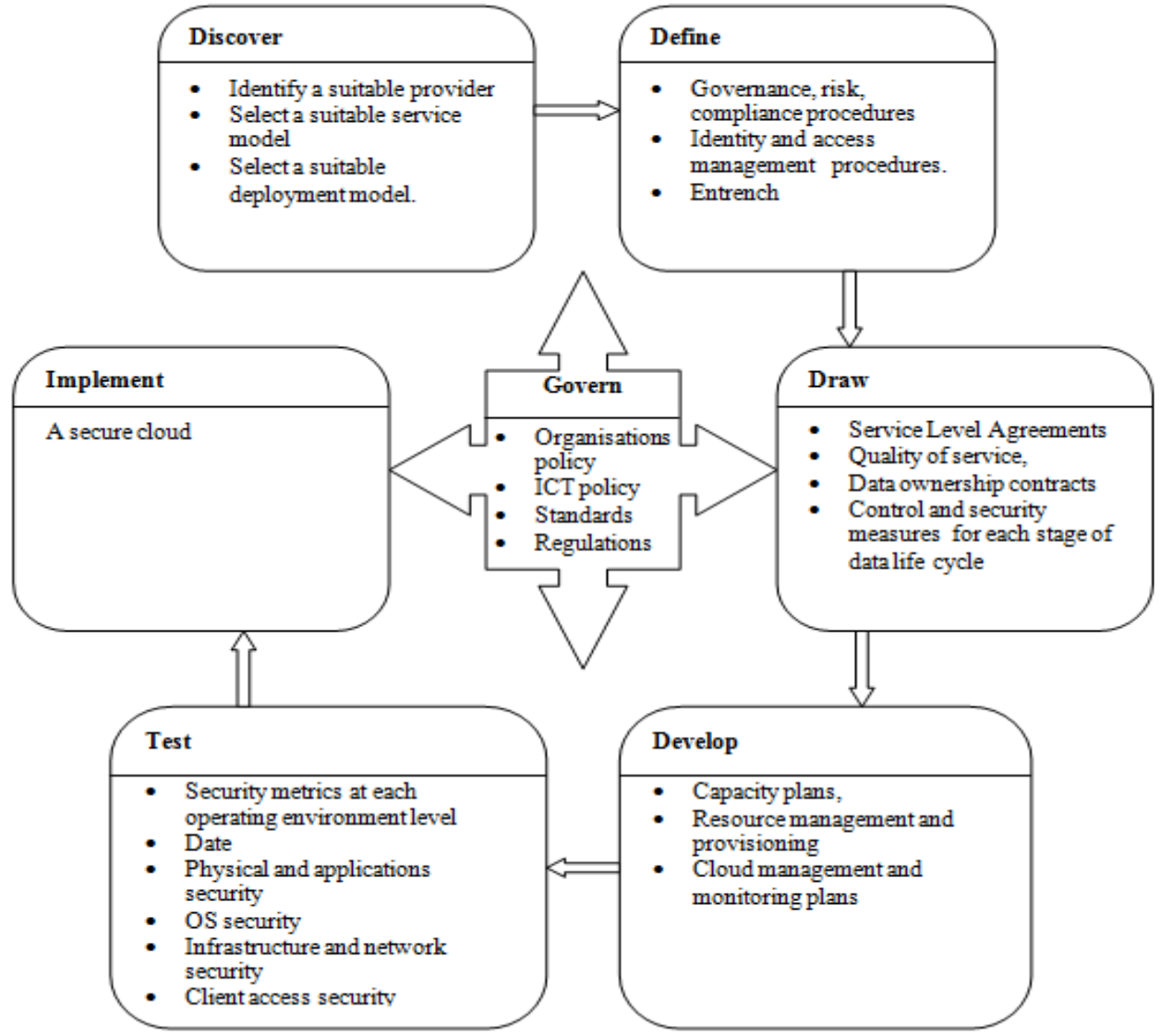
From the previous frameworks, the critical review and the results of the data collection, it is clear data security is a major concern when parastatals want to implement cloud technologies in their organisations. This chapter seeks to meet this identified need using a structured approach when it comes to the implementation of cloud computing technologies while ensuring data security.

5.2 Proposed Framework

The framework proposed by the author is as indicated in the Figure 5.1. The author proposes a six stage cloud data security model namely discovery, define, draw, develop, test and implement. Discovery entails identifying a suitable cloud service provider, selecting a suitable service model and selecting a suitable deployment model. Define entails defining governance, risk, compliance procedures, defining identity and access management procedures. Draw service level agreements, quality of service, data ownership contracts, control and security measures for each stage of data life cycle. Develop capacity plans, resource management and provisioning, cloud management and monitoring plans. Testing security metrics at each cloud operating level and each stage of data life cycle to address data security in the cloud and finally, implementing the cloud solution.

Figure 5.1: Proposed Cloud Data Security Implementation Model

.



The proposed framework has considered a number of factors from results of the data collected, previous studies and frameworks that are in place. From the results of the data analysis it was evident that GPs need a cloud data security framework with the ability to guide them on CSP selection, service, deployment models selection, GRC procedures, IAM procedures, contracts, resource and cloud management, cloud layers and data life cycle security and having a governance platform with policies, standards and regulations. From the study, the framework includes some of the key concerns related to cloud security as identified by (Gonzalez et al., 2012). Gonzalez et al (2012) classified the concerns into a model of seven categories. Cloud data security implementation model (CDSM) dwelt on six of these

categories namely: Network security, data security, virtualization, governance, compliance and legal issues. Mircea (2012) indicates that to ensure data security it requires the identification and analysis of the risks and security measures/techniques that can be applied in every stage of data life cycle. The omission of one of the stages, at least in the case of the sensitive data for organization, may lead to important loss for the organization. CDSM incorporated control and security measures of all the stages of the data life cycle. An organization security posture is characterized by maturity, effectiveness, and completeness of the risk adjusted security controls implemented. CSA (2011) identifies risk adjusted security controls implemented in three layers ranging from facilities (physical security), to network infrastructure (network security), to applications and information (application security) while Mircea (2012) identifies five security level control system in addition to CSA (2011) layers include date, OS security and client access and thus the author incorporated them into the framework.

To facilitate further studies (Gonzalez et al, 2012) organizes the information related to cloud. The main problems are identified and grouped into a model composed of seven categories: network security, interfaces, data security, virtualization, governance, compliance and legal issues. Six of the seven categories have been incorporated in the framework.

Several key references were employed to gather the information required for building these categories, including CSA's security guidance and top threats analysis, ENISA's security assessment and the cloud computing definitions from NIST. Emphasis is given on the distinction between services in software (SaaS), platform (PaaS) and infrastructure (IaaS) which are commonly used as the fundamental basis for cloud service classification and as observed by (Ramgovind, Eloff and Smith, 2010) the type of the cloud model implemented determines the level of security of a cloud computing solution. Frost and Sullivan (2010) CSP checklist is also included as a guideline in the selection of a suitable cloud service provider.

Looking at the mapping model of cloud, security and compliance(CSA) the proposed framework has added security control model.

The proposed framework also has the multitenancy function of the cloud multitenancy Model of NIST which ensures that whether business or client is on public or private cloud models, on premise or off premise security is guaranteed.

5.3 Validation

The study engaged three IT professional to validate the model. One (Evaluator 1) was an education network staff whose organisation manages cloud services for higher learning institutions. They mainly implement IaaS solution, the second (Evaluator 2) works for a government parastatal which has

implemented Email as a service solution and the third (Evaluator 3) also works with government institution which has implemented Platform as a service solution. Below are there responses as captured by the author:

5.3.1 Evaluator 1

"A data security model is a good tool for use in cloud implementation since cloud computing is a relatively new technology, there is no one standard to in use. This is one of the major reasons why cloud adoption is slow. We are a government's national research and education network (NREN) that was formed to serve higher education and research institutions in Kenya. We provide high speed internet connectivity, network training and application, web hosting, E-mail, disaster recovery, top level domain registration. We implement IaaS for our members. The IaaS consists of virtual machines, storage, virtual infrastructure database environment, a complete Linux environment. We have various data centres, some act as the backup in case of downtime or failure. All our data centres are located locally and we offer a community cloud to our members. We also run a private cloud for our systems. Some of our members cloud are on-premise and while others are off-premise. We offer security for the OS, infrastructure, and databases and the members manage their application, access control and internal security. On our cloud we have identity and access management which entail authorisation, authentication using one-factor and digital signatures. We do not use Encryption since members manage and handle their data and apply security measures of their choice. One challenge has been low levels of SLA support and standards by commercial operators and lack of reliable backup supply to member institutions. We offer shared services to save members from having to individually purchase expensive resources such as ERP (Enterprise resource planning) applications. Most of the member institutions especially new members do not have the technical capacity to host and administer their own ICT applications and services and to individually provide security and disaster recovery services. The members benefit from bulk joint procurements of teaching and administrative applications and software licenses as a way of reducing the total cost of ICT services for members. The framework will be of benefit since it identifies policies, standards once implemented in an organisation form the basis to a secure cloud environment. We have been in the forefront in the development of the National ICT policy especially in education though institutions lack ICT policy. We are influencing the formation of ICT policy and structure at institutional and national levels."

5.3.2 Evaluator 2

"I'm excited about having a cloud security framework since it is evident that there lacks standards and regulatory guidelines in the implementation of the cloud especially in the government and thus a slow uptake of the technology in the government institutions. I work for one of the government parastatal. We have a hosted solution for email services together with associated collaborative systems for meeting scheduling and task/project management. The top officials have problems accessing their locally hosted email when on trips out of the country. We are also trying to get the county and sub county officials in the ministry who are spread out throughout the country into the email system. One of the greatest fears has been the possibility of confidential email messages leaking either inadvertently or through malice. This may expose state secrets! The ministry also relies on emails for day to day operations and would not want a situation where the system is down or where support cannot be guaranteed in case a cabinet minister forgets his/her password! The emails are hosted in Europe and are managed and controlled by a government ICT regulator. The solution is deployed in a community cloud model since the regulator manages Emails for many government ministries. The SLA obligations are between the regulator and the CSP. Separate ministries and departments provide for the connectivity. A challenge has been experiencing service outage where the connectivity provider and the service provider both claim the other is at fault! There is lack of service transparency since the user would not know how the system operates and when failures occur the user reports to the regulator which informs the provider and the resolution may take long. Cloud transparency especially in security would entail cloud providers disclosing adequate information about their security policies, design, and practices, including disclosing relevant security measures in daily operations thus the model come in very handy demarcating the boundaries of all the parties including the third party who may be sidelined by this contractor hence lacking important information about the client or CSP thereof."

5.3.3 Evaluator 3

"We are a group of the staff of the larger IT department of a government parastatal involved in software development. Our institution has not adapted to the cloud technology due to security matters that have not been streamlined owing to the sensitive nature of our core business. However the institution is undertaking a thorough study on implementing a new system on the cloud which is to be used as prototype before other cloud based systems are implemented. We have implemented a Paas solution with Microsoft which provides us with a virtual machine, development frameworks and azure (Azure is a Microsoft cloud offering that has three components: Windows Azure (which provides developers with on-demand compute and storage to host, scale, and manage Internet or cloud applications), SQL Azure

(which extends the capabilities of Microsoft SQL Server into the cloud as a Web-based distributed relational database) and Azure .Net Services (which include a set of Microsoft hosted, highly scalable, developer-oriented services that provide key building blocks required by many cloud-based and cloud-aware applications). We use the platform for development of software then deploy the application into our infrastructure. The provider provides an SLA though the SLA seems to be one sided since you agree to the terms and the conditions of the service provider and they can manipulate the SLA in their favour. The service is deployed on public cloud and the users maintain access rights and control to their platform. The service is billed as per use. The cloud data security model will be beneficial to government institutions because it will instil some level of assurance in terms of data security and inform the users their roles and measurement metrics to various features in the service they are provided. ”

Table 5.3 Model Validation

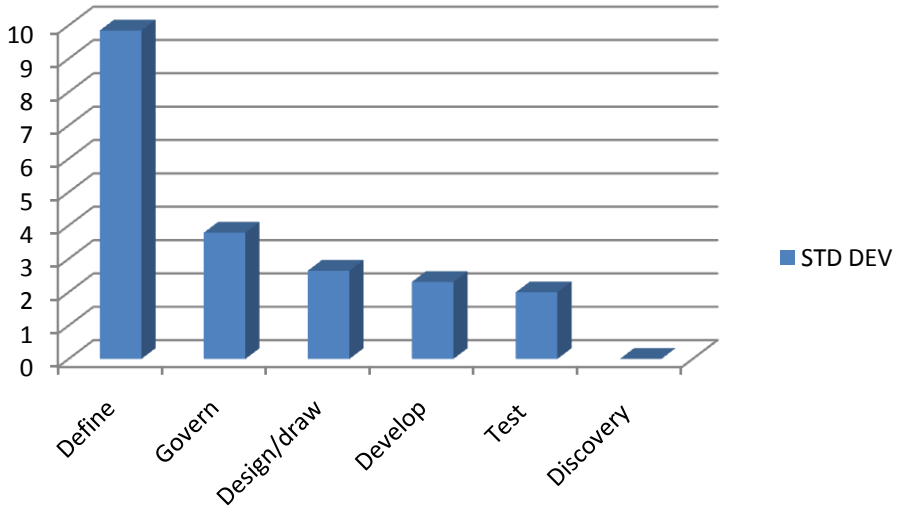
Model Component	Evaluator 1	Evaluator 2	Evaluator 3	Mean Score	Max	%	Variance	Std Dev
Discovery	8	8	8	8	8	100	0	0
Define	59	40	45	48	68	70.58824	97	9.848858
Design/draw	30	35	31	32	36	88.88889	7	2.645751
Develop	10	6	6	7	24	30.55556	5.333333	2.309401
Test	26	28	30	28	30	93.33333	4	2
Govern	12	6	5	8	12	63.88889	14.33333	3.785939
TOTAL	145	123	125	131	178	73.59551	148	12.16553

The validation form consisted of the models main components, subcomponents, risk or activities or details associated with the subcomponent and the measurement metrics. The evaluator was expected to tick to either yes, planned, no, unaware or not applicable.

This was to inform the study if the CSP of the various cloud users have applied these components in their cloud services and gauge the usability and validity of each sub component of the model. The results of the validation have been depicted in table 5.3 above where each component was assigned the total score and different evaluators scores was compared, most evaluator scored differed because they have implemented different services with different provider for different function. The author used the scores to compute the mean score, against the maximum score and a percentage of the same. The standard deviation showed how the organisations varied and the define stage had the highest variation followed by the govern stage showing that some organisations lack some of the aspects relating to Governance, risk, compliance, identity and access management , policies, standards, and regulations. In this other stages the variations

were somewhat low and thus meaning that most of them had almost or the same aspects in discovery, design/draw develop and test stages as depicted in the figure 5.2 below.

Figure 5.2 Standard Deviation of the CDSM main components



The percentage mean score of all the evaluators amounted to 73.5%. With a 74% score, there is some work to be done to get the 90% threshold set by the author! Table 5.2 first takes the components of the model which are broken down into risk area or activities or details and measurements metrics that an organisation can use to determine how well the CSP is prepared to take care of the security issues associated with cloud computing. The score is simplified into availability of a solution or mitigating factor (yes), non-availability (no) and possible availability in the foreseeable future (planned). Since these are just guidelines, the organisation will have to determine how detailed CSP will to be prepared to meet the customer's requirements.

The study suggests a score of two(2) points if the answer to a query is 'Yes', a score of one(1) point if the answer is 'planned' and score of zero(0) if the answer is 'no' or Not Applicable(N/A). The total scored divided by the total possible score of will enable one to work out the percentage that is indicative of how secure your cloud data is.

Table 5.2 Cloud data security evaluation table

In the following evaluation table, the evaluator checks the framework component and sub components and indicate whether it is covered [yes], planned [planned], not covered [NO] and not applicable [N/A] by the cloud service provider (CSP).

No	Framework Component	Sub component	Risk Area	Details Score	Measurement Metrics	Score			
						Yes	Planned	No	N/A
D1	Discovery	Cloud service provider	Develop a check list for CSP selection, analyse provider profile internal processes and procedures.	It's important to consider various factors in selecting the CSP such as data centre location, security features, data handling policies e.t.c.	Checklist Internal processes and procedures transparency. Periodically assess providers risk profile.	☐	☐	☐	☐
D11		Service model	Selection procedure management and control issues	Prospect cloud customers should undertake proper due diligence on providers before entering into a formal relationship	Detailed due diligence investigations provide unbiased and valuable insight into provider past track record including financial status, legal action taken against an organisation and its commercial reputation.	☐	☐	☐	☐
				Three general areas are used to measure cloud service, they are	Service Measurement Index (SMI), could be used to	☐	☐	☐	☐

				service selection, service agreement and service verification.	determine which metrics are relevant to the selection of a particular cloud offering.				
D12		Deployment model	Selection procedure management and control issues	The deployment model included in the CSA should clearly specify one of the following options: Private, Community, Public, or Hybrid.	Customers must be well educated on the characteristics and differences in each of these deployment models since potential value and risk varies significantly.	□	□	□	□
D13					Component Subtotal (8/12)				

No	Framework Component	Sub component	Risk Area	Details Score	Measurement Metrics	Score			
						Yes	Planned	No	N/A
D21		Governance procedures	Insufficient governance Difficulty in addressing stronger privacy and regulatory mandates.	Dependence on external entities causing untimely response to security incidents and implementing systematic business continuity and disaster recovery plans.	Establish or adopt a cloud security governance framework for cloud management and control.	□	□	□	□
				Issues related to loosing administrated	Assess the provider's security governance processes and capabilities for sufficiency, maturity, and consistency with the customer's information security management processes.	□	□	□	□
D22		Risk mitigation procedures	Uncertainty in enforcing security policies and inability to support compliance audits in the cloud.		Re-evaluate existing lifecycle models, risk analysis and management processes testing and service attestation.	□	□	□	□
					Due diligence to take place on cloud service provider to assure customer of their security control measures and transparency.	□	□	□	□

D23		Compliance procedures		Compliance includes requirements related to service availability and audit capabilities.	Insight into the inner workings and risk profile of cloud providers processes and applications for assuring IT governance and demonstrating due diligence.	□	□	□	□
					Validation and verification activities that assure that the CSP is practises following claimed security and risk management strategies properly tacks due care on to due diligence.	□	□	□	□
D24		Identity and access management	AUTHORISATION	These apply to the cloud provider's identity and access management systems (those under their control)	The accounts with the highest level of privilege authenticated and managed properly.	□	□	□	□
					The most critical decisions (e.g., simultaneous de-provisioning of large resource blocks) are authorised according the SOPs.	□	□	□	□
					The segregation of duties is observed.	□	□	□	□
					Role-based access control (RBAC) and the principle of least privilege followed is followed.	□	□	□	□

					Changes, if any, made to administrator privileges and roles to allow for extraordinary access in the event of an emergency are well documented.	□	□	□	□
					There is an 'administrator' role for the customer e.g. customer administrator has a role in adding new users.	□	□	□	□
D241			Identity provisioning	Checks should be made on the identity of user accounts at registration.	There are different levels of identity checks based on the resources required.	□	□	□	□
D242			Management of Personal data		Data storage and protection controls apply to the user directory (e.g., AD, LDAP) and access to it.	□	□	□	□
D243			Key management	For keys under the control of the cloud provider, security controls are in place:	Security controls are in place for reading and writing those keys.	□	□	□	□

				For example, strong password policies, keys stored in a separate system, hardware security modules (HSM) for root certificate keys, smart card based authentication, direct shielded access to storage, short key lifetime.	Procedures in place in the event of a key compromise. For example, key revocation lists.	□	□	□	□
D244		ENCRYPTION	Insecure Cryptography	Cryptography algorithms usually require random number generators, which use unpredictable sources of information to generate actual random numbers, which is required to obtain a large entropy pool. If the random number generators are providing only a small entropy pool, the numbers can be brute forced.	Attribute-Based Encryption Algorithm such as Cipher text-policy ABE (CP-ABE) In the CP-ABE, the encrypt or controls access strategy, as the strategy gets more complex, the design of system public key becomes more complex, and the security of the system is proved to be more difficult. Key-policy ABE (KP-ABE) In the KP-ABE, attribute sets are used to explain the encrypted texts and the private keys with the specified encrypted texts that users will have the left to decrypt.	□	□	□	□
			Encryption can be used	There is a well-defined policy for what should be encrypted and what	Fully homomorphic encryption (FHE) such as Searchable				

			in multiple places – Data in transit Data at rest Data in processor or memory Usernames and passwords	should not be encrypted, the key holder(s) and the protection for the keys.	Encryption (SE)				
D245		AUTHENTICATION	What forms of authentication are used for operations requiring high assurance? This may include login to management interfaces, key creation, access to multiple-user accounts, firewall configuration, remote access, etc.	Two-factor authentication used to manage critical components within the infrastructure, such as Firewalls.		□	□	□	□
D246		CREDENTIAL	The CSP provides anomaly detection (the	Anomaly detection in place		□	□	□	□

		COMPROMISE OR THEFT	ability to spot unusual and potentially malicious IP traffic and user or support team behaviour). For example, analysis of failed and successful logins, unusual time of day, and multiple logins, etc.						
				Provisions exist in the event of the theft of a customer's credentials.		□	□	□	□
D247		IDENTITY AND ACCESS MANAGEMENT SYSTEMS	This refers to the identity systems offered to the cloud customer.	The CSP is interoperable with third party identity providers?		□	□	□	□
D248		ACCESS CONTROL		The client credential system allows for the separation of roles and responsibilities and for multiple domains (or a single key for multiple domains, roles and responsibilities)		□	□	□	□

				Single sign-on can be incorporated.					
		ACCESS CONTROL		The client credential system allows for the separation of roles and responsibilities and for multiple domains (or a single key for multiple domains, roles and responsibilities).		□	□	□	□
				Access to customer system images is managed ensuring that the authentication and cryptographic keys are not contained within in them.					
				There mutual authentication when the customer sends API commands or when the customer logs into the management interface.					
D249		AUTHENTICATION		CSP supports a federated mechanism for authentication.		□	□	□	□
				Cloud provider infrastructure be located in the same country.		□	□	□	□
D25	LEGAL PROCEDU	CSP customers should have regard to their respective		The cloud provider will use other companies whose infrastructure is located outside that of the cloud		□	□	□	□

	RES	natural and international obligations for compliance with regulatory frameworks and ensure any such obligations are appropriately complied with.		provider.					
				The jurisdiction over the contract terms and over the data will be the same.		□	□	□	□
				The cloud provider's services be subcontracted out /outsourced.		□	□	□	□
				The data provided by the customer and the customer's customers, be collected, processed and transferred with due regard to the data privacy laws.		□	□	□	□
				The data sent to the cloud provider will remain the customer's intellectual property upon Termination of the contract.		□	□	□	□
					Component Subtotal ( )				

No	Framework Component	Framework sub component	Risk Area	Details Score	Measurement Metrics	Score			
						Yes	Planned	No	N/A
D3	DRAW	SLA	Establish policies and procedures in the selection of the cloud provider.	Cloud security controls and scopes are negotiated into contracts for service , quality, service levels, privacy, ownership and compliance This issues are dealt with legally	Security policy and controls are applied (contractually) to the Cloud providers?	□	□	□	□
					Legal precedence for agreement breaches.	□	□	□	□
					Templates in the cloud SLA makes it easier and faster to define a cloud SLA and service level objectives	□	□	□	□
D31					Ability to assess risk profiles of third party cloud provider	□	□	□	□
					Protection requirements for information and computer systems, security bleaches, disclosure laws regulating requirements privacy requirements and international laws.	□	□	□	□

D32		QOS	Detail the procedures used to assure third parties accessing your infrastructure (physical and/or logical).		Outsourcers and subcontractors audited in a scheduled and ad hoc manner.	□	□	□	□
D33		Data ownership		SLA provisions guaranteed by outsourcers equal or higher than the SLAs CSP offer to customers.	Measures are taken to ensure third party service levels are met and maintained with supplier redundancy in place	□	□	□	□
D34	Security procedures in each stage of the data lifecycle								
D341		Creation	Establish the policies and procedures for access.	Data security on creation supposes the generation/ discovery and actualisation of digital content.	Authentication and authorisation of users, applications and databases. Separation of responsibilities, roles access log and ACLS.	□	□	□	□
					Privileged user access and administration security solutions such as access management and data encryption.	□	□	□	□
D342		Storage	Establish policies and procedures for back up	Data storage can take place in internally, externally, public, private or hybrid locations. Their security requires information about the storage locations security	Encryption of data at rest and in motion / transit	□	□	□	□

				technologies.					
D343		Sharing	Establish policies and procedures for sharing	Data sharing is expanding the use range of the data and renders data permissions more complex. The data owners can authorize the data access to one party, and in turn the party can further share the data to another party without the consent of the data owners.	Key management, sharing policy, maintenance of the original protection measures and usage restrictions.	□	□	□	□
D344	Security procedures in each stage of the data lifecycle	Use	AUDITLOGS are used in the event of an accident requiring investigation. They can also be used for troubleshooting. End customer will need assurance such information that in available.	Can the CSP detail what information record is recorded within audit logs?	Segmentation of data within audit logs possible.	□	□	□	□
				What controls are employed to protect logs from unauthorised access or tampering?	Controls exist to protect logs	□	□	□	□
				What methods are used to check and protect integrity of audit logs?	Audit log verification method exists.	□	□	□	□

				When are the audit logs reviewed?	There exist recorded events that result in action being taken.	□	□	□	□
D345		Maintain	Data disclosure to unauthorised systems or personnel.	Metadata of network and applications should be considered recorded e.g. network perimeter devices such as firewalls, (virtual) switch, router, load balancer e.t.c. The format in which data is stored.	Measures to control how and who access organisational data	□	□	□	□
					Data protection using cryptographic mechanisms such as encryption or hashing . Key management systems	□	□	□	□
D346		Deletion	Provision for additional data storage requirements need to be estimated and planned for.	Data classification promotes establishment of data strategies and risk profiling.	Verification of data disposal mechanisms thus no remanance such as overwriting.	□	□	□	□
					Component Subtotal				

No	Framework Component	Framework Sub-component	Risk	Outputs	Measurement Metrics	Score			
						Yes	Planned	No	N/A
D5	Develop	Capacity plans	Establish whether the cloud provider	Define those services that are outsourced or	The number of unplanned resources required to provide adequate	□	□	□	□

			subcontracts some operations that are key to the security of the operation to third parties plus third parties with physical or remote access to the cloud provider infrastructure.	subcontracted in the service delivery supply chain that are important to the security (including availability) of your operations.	capacity.				
					The percentage of accuracy of the actual versus planned as given in the capacity plan	□	□	□	□
					The percentage of over capacity, The number of new or changed services implemented without capacity or performance- related issues.	□	□	□	□
					The actual business demand as a percentage of forecasts of demand.				
D51		Resource management and provisioning		Detail the procedures used to assure third parties accessing your infrastructure (physical and/or logical).		□	□	□	□
SC3		Cloud management and monitoring plans		SLA provisions guaranteed by outsourcers equal or higher than the SLAs CSP offer to customers.		□	□	□	□
					Component subtotal ( )				

No	Framework Component	Framework Sub -component	Activities/Details	Measurement Metrics	Score			
					Yes	Planned	No	N/A
D5	Test	Date	Controls used to protect the integrity of dates and time. What time source is used to synchronize system and provide audit log time stamping.	Access control list and log are maintained. System time for audit log can be set according to the customers desires.	□	□	□	□
D51		Physical security	Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption.	Serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers. Obstacles can be placed in the way of potential attackers and sites can be hardened against accidents and environmental disasters. Such measures can include multiple locks, fencing, walls, fireproof safes, and water sprinklers. Surveillance and notification systems can be put in place, such as lighting, heat sensors, smoke detectors, intrusion detectors, alarms, and cameras. Methods can be implemented to apprehend attackers (preferably before any damage has	□	□	□	□

				been done) and to recover quickly from accidents, fires, or natural disasters.				
SC3		Application/ software security	Controls used to protect integrity of applications /software used. Do they have practise to keep safe?	Measures are taken to ensure Security standards and procedures are followed.	□	□	□	□
			Software release penetration test to ensure it does not contain vulnerabilities. If vulnerabilities are discovered whats the process for remedying this? Patch management covers all layers of cloud delivery technologies i.e.(Network, server OS, virtualization software, application and security subsystems(firewall, antivirus gateway, intrusion detection systems e.t.c)	Using of tools such as rational appscan tool which scans vulnerabilities in web services such as a cloud security service (i.e. IBM cloud initiative)	□	□	□	□
				Details of the patch management procedure are available.	□	□	□	□
		OS security	The use virtualization technology brings about risks associated with multitenancy, VM isolation, hypervisor vulnerabilities	Special malware protection, IDS/IPS, firewalls, and networking protection software. CSPs must also use a security management solution that can span both the physical and virtualized elements of the IT infrastructure.	□	□	□	□

		Infrastructure security	Invisibility and disintegration of familiar security controls	Improve transparency and ability to integrate security controls especially at the network layer.	□	□	□	□
		Network security	Identify the control used to mitigate DDOS(distributed denial of service)	Defence in depth methods used e.g. deep packet analysis traffic throttling, packet black holing, capacity planning, redundancy and back up performance and uptime requirements in SLA e.t.c.	□	□	□	□
				Defences against ‘ internal (originating from CSP networks) attack as well as external(originating from the internet or customer attacks) attacks exist.	□	□	□	□
		CSP network security	The CSP should provide levels of isolation that are used for virtual machines physical machines, network storage, management networks and management support systems e.t.c	Isolation exists for virtual machines, physical machines, networks and storage	□	□	□	□
			The network architecture should support continued operation from the cloud when the company is separated from the service provider and vice versa (e.g. is there a critical dependency on customers LDAP systems.)	The architecture supports continued operation from the cloud when the company is separated from the service provider.	□	□	□	□
				CSP ensures virtual images are hardened by	□	□	□	□

				default.				
				The hardened image is protected from unauthorised access.	□	□	□	□
			The virtual systems need to be hardened.	The CSP firewall is run with only minimum ports necessary to support the services within the virtual distance.	□	□	□	□
			Minimise the ports used.	The host based intrusion prevention service(IPS) can be run in the virtual distance.	□	□	□	□
		Client access security	unauthorised disclosure, or alteration, of confidential or sensitive agency data		□	□	□	□
				Component Subtotal ( )				

No	Framework Component	Activities/Details	Outputs	Measurement Metrics	Score			
					Yes	Planned	No	N/A
01	Organisations /ICT policy	Establish information security requirements from organisation organisations policy, legal and regulatory obligations. Uncertainty in enforcing security policies at the provider's site and their inability to support compliance.	Information security requirements may carry through from other contractor SLA	Security policy and controls are applied (contractually) to the third party providers?	□	□	□	□
				Analyse the risk profile of the third party providers	□	□	□	□
02	Standards	Develop standards to ensure deployment and adoption of secure clouds.	Identify standards that provide consistency in metric definitions and methods of collection.	Certifications schemes such as ISO27001 provide customers with assurances the CSP has considered, its management of information security risks.	□	□	□	□
				Well structured cyber insurance industry.	□	□	□	□
03	Regulations			Advocate for adequate governance frameworks and regulations	□	□	□	□

				Verify existence of adequate protection mechanisms.	□	□	□	□
				Component Subtotal ( )				

The framework was received very positively and with a lot anticipation that with some customisation in respect to the organisation it would be of great help to cloud adopter in the government sector. Suggestions were put forward such as to add training in the develop stage in order to build capacity for users and CSP employees.

5.4 Summary

Frameworks such as CDSM make significant impact and create healthy competition among Cloud providers to satisfy their Service Level Agreement (SLA) and improve their Quality of Services (QoS). It is important to note that as stated by Becker and Bailey (2014) no one framework or model encompasses all of the possible IT controls, collectively they cover the "what, how, and scope" of IT Governance.

Chapter 6

Conclusions and Recommendations

6.1 Summary

Cloud computing offers many opportunities to organizations, but risks and challenges as well. For an organisation to succeed institutions must critically examine available data, create policies especially security policies, follow existing standards and develop adequate procedures of ensuring adherence. This study offers a means for GPs to implement cloud solutions in a more secure way, though it is not exhaustive but an approach that is oriented on most of the stages that an organisation must go through to achieve a relatively secure cloud environment.

6.2 Conclusions

Cloud computing present different risks to an organisation than traditional IT solutions. As use of cloud are scaled up to larger and larger systems, it is becoming extremely important to find effective models for cloud security before deploying to a larger scale in any organisation.

The study had a response rate of 76%, the results found are in line with past results in other studies. The objectives of the study were met. It was able to analyze the service and deployment models implemented in government parastatals, the results showed that most GPs have implemented IaaS followed by software as service (SaaS) and storage as a service. However, Most GPs combine cloud services in addition to the main cloud service (such as Iaas, and then add backup as a service among others). Private cloud model is the most prevalent cloud model deployed by almost 70% of the GPs followed by the hybrid cloud model. Only 7% of the GPs have deployed their systems in public cloud and /or community model. This is because cloud model is perceived to be easier to align with security, compliance and regulatory requirements in addition to an organisation achieving overall control and use.

The research was able to analyze cloud computing security challenges and/or threats affecting GPs currently and techniques for protecting data in the cloud for government parastatals. All the challenges analysed had some level of effect to the organisation. The first ten challenges and/or threats were selected based on the threat/ challenge with the greatest effect. They include 1) Malware, 2) Uninterrupted availability, 3) Data loss(remanence), 4) Cloud bursting, 5) Provider profile unknown risk 6)Legal issues 7)Cracking, 8) Hijacking of accounts, services and traffic 9) Regulations and finally 10) Denial of service. Table 4.13.2 highlights the techniques to be employed to protect data against the above challenges.

The research found that GPs do not have a specific governance framework involving cloud data security in use and policies. Less than 30% adhere to governance framework, 40% do not have and the rest do not know which framework they are using. Statistics showed that only 14% of the GPs use COBIT, 18% use COBIT combined with ITIL and ICT policy, and the rest use other frameworks or standards. It was evident that most of them had little knowledge on the cloud frameworks and standards governing their cloud solutions.

From the analysed data and literature reviewed, a cloud data security implementation model for government parastatals was designed. The model will play a pivotal role in ensuring implementation of a secure cloud solution in GP. The proposed model components informed by different features from other documented cloud security model such as Cloud Multi-tenancy Model(CMM) of NIST, Cloud Risk Accumulation model (CRAM) of CSA, Cloud Cube Model(CCM) of Jericho and standards such as ENISA, ISO27001and ISO27002, CCIAF, ITIL and ISACA. It is composed of six stages namely: discovery, define, design/draw, develop, test and implement. The proposed model was evaluated and proven to work with little customization owing to the difference in the functions or the cloud solution being undertaken. The model includes measurements of both organizational and technical issues related to keeping cloud services at an acceptable level of information security and data privacy. This includes ensuring security of sensitive data held by governmental parastatals.

6.3 Recommendations for Future Research

The model is recommended for use in government parastatals and it acts a guideline ensuring that security is integrated while implementing the cloud solutions.

The respondents of this research were selected randomly and thus may not give a true reflection of the cloud computing scene. A more stratified approach will need to be used taking into account the role, industry, company size and other relevant factors to be able to get a clearer picture of cloud computing phenomena and its associated risks. It is the researcher's recommendation that:

1. More should be carried on the vulnerabilities affecting virtualisation and their mitigating factors

2. The government to have national cloud policy, laws and standardised SLA to prevent cloud clients from exploitation since CSP have an upper hand and secretion in implementing the SLA.

3. More research should be carried out in the area of cloud computing and how it can help propel developing countries like Kenya.

4. More investigation can be carried out on the cloud security models and involvement of IT employees in the implementation of cloud technologies in public institutions.

References

Alzain, M., Soh, B. and Pardede, E. (2012) 'A New Approach Using Redundancy Technique to Improve Securit in cloud computing', *IEEE*.

Avison, D. and Heje, P.- (2005) Research in information systems. A handbook for research supervisors and their students, Heinemann, Oxford: Elsevier Butterworth.

Barinder, K. and Sandeep, S. (2014) 'Parametric Analysis of various Cloud Computing Security Models', *International Journal of information and Computation Technology.*, vol. 4, no. 15, 2014, pp. 1499-1506.

Becker, J.D. and Elana, B. (2014) 'IT Controls and Governance in Cloud Computing', 20th Americas Conference on Information systems(AMCIS), Savanah.

Bernice, K., Partner, Cassels, Brock and Blackwell, L. (2011) 'Data security- The Case against Cloud Computing', March 2011.

Catteddu, D. and Hogben, G. (2009) 'Cloud computing: benefits, risks,and recommendation for information security', *European network and information security Agency*.

Cheng, F. C.; Lai, W. H.; (2012) The impact of cloud computing technology on legal infrastructure on legal infrastructure within internet focusoing on the protection of information privacy, Procedia Engineering.

Cloud Ctandards Customer Council (2012) 'Security for Cloud Computing: 10 steps to ensure Success '.

CSA (2011) 'secuirty guidance for critical areas of focus in cloud computing', *Cloud Security Alliance*, vol. 3.0.

Daniele, C. and Giles, H. (2009) 'cloud Computing Information Assurance Framework', *ENISA*.

Dargha, R. (2011) Cloud computing: Key considerations for adoption, Bangalore, India: Infosys.

Dooley, B. (2010) 'Architechtural requirements of the hybrid cloud', *information mangement online*.

Fowler, F.J. (2002) *Survey research methods*, 3rd edition, Thousand Oaks, CA: Sage publications.

Fran, H. (2012) Best practises for cloud security. how security in the cloud can be a better bet than doing it yourself, Bloor Research white paper.

Gens, F. (2009) 'New IDC IT cloud services survey: Top benefits and challenges", *IDC Exchange*.

Gonzalez, N., Miers, C., Carvalho, T., Simplicio, M., Naslundy, M. and Pourzandiy, M. (2012) *A quantitative analysis of current security concerns and solutions for cloud computing.*, Stockholm, Sweden, Sao Paulo Brazil: Erricsson Research.

Hashizume, K., Rosado, D. and Fernadez-Medina, E. (2013) 'An analysis of security issues for cloud computing', *Journal of internet services and applications*, no. 10.1186, p. 2.

Hp (2013) 'Securely enable the cloud'

Kent, B.H., Singleton, J.C. and Veit, E.T. (2010) survey reaseach in corporate finance: Bridging the gap between theory and practise, Oxford university press.

Ko, R., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q. and Lee, B.S. (2011) 'Trustcloud: Aframework for accountability and trust in cloud computing', *IEEE ICFP*, 2011.

Leavitt, N. (2009) 'Is cloud computing really ready for prime time?', *Computer*, vol. 42, 2009, pp. 15- 20.

Luna, J., Ghani, H., Germanus, D. and Suri, N. (2012) 'A security metrics framework for the cloud department of computer science ', *Technische Universit'' at Darmstat Hochschulstr , Germany*, vol. 10, no. 64289.

Macias, F. and Greg, T. (2011) 'Cloud computing concerns in the public sector- How government, education and healthcare organisations are assessing and overcoming barriers to cloud deployments.'.

Malik, A. and Nazir, M.M. (2012) 'Security framework for cloud computing environment: A review', *Journal of emerging trends in computing and information sciences.*, vol. 3, no. 3, March 2012.

Mano, P. (2011) 'Security in the skies: Cloud computing security concerns, threats and controls', *Institute of Computer security(ICS)*.

Mircea, M. (2012) 'Addressing Data security in the cloud.', World Academy of Science, Engineeringand Technology, International science index 66, vol. 66, June 2012.

Mugenda, O.M. and Mugenda, A.G. (2009) *Research methods Quantitative and qualitative approaches*, Nairobi: Acts Press.

Omwansa, T.K., Waema, T.M. and Omwenga, B. (2014) 'Cloud computing in Kenya: A 2013 baseline survey', *University of Nairobi, school of computing and informatics & computing for development Lab(C4DLab)*, April 2014.

Popovic, K. and Hocenski, Z. (2010) 'Cloud computing security issues and challenges', *MIPRO*, no. 10, December 2009, pp. 15-20.

Project management institute (2012) 'Cloud computing: The new strategic weapon White paper'.

Ramgovind, S., Eloff, M.M. and Smith, E. (2010) 'The management of security in cloud computing, School of computing, Universit of South Africa, Pretoria', *IEEE*, 2010.

Ritesh, G.A., Chatur, P.N. and Swati, G.N. (2012) 'Cloud Computing and Security Models: A survey', *Certified international Journal of Engineering, Sceince and Innovative Technology(IJESIT)*, vol. 1, no. 2, November 2012.

Sezen, A., Bostan, A. and Yazici, A. (2014) 'Security issues of cloud computing and alternative approaches', international Conference on Advanced Technology and sciences, 2014.

Shen, Z. and Tong, Q. (2010) 'The security of cloud computing system enabled by trusted computing technology.', *ICSPS*, vol. 2, 2010, pp. 11-15.

Souter, D. and Makau, M.K. (2012) 'Internet goverance in Kenya- An Assessment for the Internet Society'.

Subashini, S. and Kavitha, V. (2010) 'A survey on security issues in service delivery models of cloud computing', *Journal of network computing applications*, July 2010.

Travis, D. and Annie, I. (2008) 'Analysing regulatory rules for privacy and security requirements', *IEEE Trans. software Engineers*, vol. 34, no. 1, pp. 5-20.

Vaquero, L.M., Rodero- Merino, L., Caceres, L. and Lindner, M. (2009) 'A break in the clouds: towards a cloud definition', *ACM SIGCOMM Computer communication Review*, vol. 39, no. 1.

Victor, R.K., Sigar, O.K. and Odongo, G.Y. (2012) 'Meta-modelling cloud computing Architechture in distance Learning, department of computer science, Egerton University and Kabarack University', *International Journal of computer science issues (IJCSI)*, vol. 10, no. 3.

Weinhardt, C., Anandasivam, A., Blau, B. and Stosser, J. (2009) 'Business Models in the service World ', *IT Professional*, vol. 11, pp. 28- 33.

Wrinkler, V.). (2011) *Securing the cloud: cloud computer security techniques and tactics*, 978159749592nd edition, 225 Wyman Street, Waltham MA 02451 USA: Elsevier Inc.

Xue, J. and Zhang, J. (2010) 'A brief survey on the security model of cloud computing ', *International symp. on distributed and applications to business, engineering and science.* , 2010, pp. 475-478.

Yaser, G., Jennifer, F. and Frank, M. (2012) 'Emerging issues and challenges in cloud computing- A hybrid approach Department of Computer Science, University of Calgary, Canada', *Journal of Software Engineering and applications*, vol. 5, November 2012, pp. 923-937.

Appendix 1

Table 4.7 Data life cycle and security measures

Stage	Security measures applied in each stage
Creation	User profiling, proper content design access, validation measures, structured data gathering, authentication of identities, Type checking, access control, Secure by design, User access rights management, tagging, classification levels, Encryption, quality assurance and User IDs
Sharing	Public folders encryption and passwords, Digital certificates , Sensitivity levels (profile / account control), use Secure Socket Layers (SSL) and transport layer security (TSL) protocols, audit trails encryption - digital signature, content encryption, application security, access controls, content monitoring and protection, access rights, and Designated data leakage prevention (DLP)
Maintain	Policy guidelines, authorisation, senior personnel, logs, access control lists, passwords and change triggers, data encryption, hardening of server, content discovery, audit trails, Log records, recovery plans, Asset management, data controls, user profiles and logical controls
Storage	Tapes authorised by DBA, rights management, media and environmental controls, Backup, DR and updates passwords, encryption, logical controls access controls and log files
Usage	Policy access in place, authorised senior personnel, logs, ACLs, password, authorisation policies, physical and logical controls, recovery plans, access monitoring, enforcement, authentication, privilege levels, monitoring, user rights management and data labelling and backups
Destroy	Policy to guide in place, legal rights, disposal regulations, secure deletion archiving and tape disposals with encryption, cleaning and recovery procedures, overwriting and most data is retained.

Appendix II: Hardcopy Questionnaire

Introduction

I am an MSC student at the University of Nairobi undertaking a Master of Science degree in Information Technology Management. As part of the requirement for completion of the degree a student must undertake a research. The purpose of this questionnaire is to obtain structured input from government parastatals to help provide a solution for cloud data security when they want to adopt cloud services for their work.

Background

Cloud Computing is a distributed computing model for enabling service-oriented, on-demand network access to rapidly scalable resources Such resources include infrastructure as a service (IaaS), development and runtime platforms as a service (PaaS), and software and business applications as a service (SaaS). Clients do not own the resources, yet applications and data are guaranteed to be available and ubiquitously accessible by means of Web services and Web APIs "in the Cloud".

Cloud Computing is about improving organizational efficiency and reducing cost, often coupled with the objective of achieving a faster time-to- market. Centrally hosted services with self-service interfaces can help to reduce lead times between organizational units who use the cloud as a collaborative IT environment.

Re-usable components, packaged on virtual machines, provide a way to exchange working IT solutions. Capabilities to allocate and de-allocate shared resources on demand can significantly decrease overall IT spending. Low-cost access to data centres in different geographical regions may further reduce market entry barriers and enable new business models.

As the public sector gears to adopt to cloud computing considering the value preposition mentioned above there are grievous security concerns among others that hinder fast uptake of the technology by the public sector. They include data security, data loss/leakage prevention, access controls abuse and nefarious use of computing resources, insecure and proprietary APIs, share technology vulnerabilities, hijacking of accounts, services and traffic, governance, regulation and compliance, cyber forensics and personnel security.

These concerns pose threats such as cracking, malware, cloud bursting, vendor lock-in, disclosure to unauthorised systems or personnel, denial of service, distributed denial of service, insider attacks, data loss and data remanence and many others. Cloud control matrix (CCM) revised by cloud security architecture (CSA) which provides fundamental security to guide vendors and can also be used b clients to assess the overall security risk of the cloud service provider. The controls include cryptographic protection, secure data disposal, overwriting of storage media data loss/leakage prevention, Access control lists(ACLs), session management, capacity planning, back up, validate and verify providers assurance controls among others.

Instructions:

This questionnaire has five sections (A, B, C, D and E). Kindly follow instructions as provided. Please read the questions and answer them either by filling in the blank spaces or ticking the check boxes [√] or selecting the option buttons(for the online questionnaire)

SECTION A: GENERAL INFORMATION

1. What is your current position in your organisation?

(i) Management [ ]

(ii) Supervisor [ ]

(iii) Employee [ ]

2. Which department are you in? ICT [ ] Finance [ ]

Any other (Specify) ……...

3. Kindly indicate the name of your organisation …….....

SECTION B: CLOUD COMPUTING ADOPTION

Cloud computing adoption refers to an organisation migrating some or all its data and applications to an external independent organisation that provides software, infrastructure and platform as a service and is paid per use.

Cloud computing uses virtualization technologies to provide on demand computing resources via networks and has the following characteristics: on-demand self-service, resource optimization, scalability,

flexible pricing model, and measured service. The flexibility of a cloud-based framework allows cloud service providers to support multiple products with shared resources. Cloud computing basically consists of three service models: (1) Infrastructure as a Service (IaaS): the provision of storage capabilities and computing power; (2) Platform as a Service (PaaS): the provision of a programmable environment with needed programming languages, libraries, services, and tools; (3) Software as a Service (SaaS): the provision of web-based applications.. Each deployment model has its benefits and drawbacks . The decision of choosing a proper cloud computing deployment model should take technological as well as organizational factors into consideration.

3. Has your company adopted cloud computing (if no to this question, go to question 4,

6 and 9 only)?

(i) Yes [ ] (ii) No [ ]

4. If no to question 3 (firm has not adopted cloud computing), how would you rate the firm's

intention to use cloud computing?

Do not intent to use cloud computing [ ]

Might consider using cloud computing [ ]

Intend to use cloud computing [ ]

5. If currently using cloud computing, kindly rate your level of satisfaction with the

service?

Very dissatisfied [ ]

Dissatisfied [ ]

Neutral [ ]

Satisfied [ ]

Very satisfied [ ]

6. Kindly indicate where you learnt (main source of information) about cloud

computing?

Not aware of Cloud Computing [ ]

Social Media [ ]

TV, Radio or Newspapers [ ]

Friends/family [ ]

School (learning institution) [ ]

Cloud providers [ ]

7. What cloud computing service does the firm currently use? (Tick all that applies)

Infrastructure as a Service (data center & storage services) [ ]

Storage as a Service (disaster recovery, security services & hosted applications) [ ]

Back-up as a Service (data archiving & backup and recovery) [ ]

Any other (specify)…….

8. Kindly indicate

i) Who manages service? Organisation [ ] Third party [ ] Both [ ]

ii) Who owns the infrastructure? Organisation [ ] Third party [ ] both [ ]

9. a) In your own opinion, would you like your organisation to migrate some of its services to the cloud.

(i) Yes [ ] (ii) No [ ]

b) If yes, kindly indicate which of the cloud services (Infrastructure as a service, Software as a service, and platform as a service) and cloud models (Private, public, community or hybrid cloud) would you advise your organisation to deploy.

Cloud service ……

Cloud model …….

10. There are basically four ways to deploy cloud computing, they include

private cloud (Cloud infrastructure for single organization only, it may be managed by the organisation or a 3rd party, on or off premise), **public cloud** (Cloud infrastructure that is available to the general public, it is owned by an organisation that sells cloud services), **community cloud** (Cloud infrastructure shared by several orgs that have shared concerns, managed by org or 3rdparty), and **hybrid cloud** (Two or more different clouds bound by standard or proprietary technology)

Kindly indicate the cloud model deployed in your institution

Private [ ] Public [ ] Hybrid [ ] Community [ ]

SECTION C: CLOUD COMPUTING SECURITY CHALLENGES AND THREATS

Data loss incidents turn into data leak incidents in cases where media containing sensitive information is lost and subsequently acquired by unauthorized party.

A data leak is possible without the data being lost in the originating side.

Cracking is a methodology for breaking into secured computer systems.

Malware (malicious software) it is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, Trojans, spyware, adware and toolkits e.t.c which steal protected data, delete documents or add software not approved by a user.

Cloud bursting is an application model in which an application deployment model in which an application runs in a private cloud or data centre and bursts into a public cloud when the demand for computing capacity spikes.

Data remanence is the residual representation of digital data that remains even after attempts have been made to remove or erase data.

11) Tick in the appropriate box to indicate the extent to which the following challenges or threat affect the security of cloud computing data and resources and indicate a possible technique to mitigate the challenges or threats. Kindly rate the extent of each matter on a scale of 1 to 4 (1 = no extent, 2 = Little Extent 3 = Moderate Extent 4 = Great Extent).

Concern	1	2	3	4
Data Security (Disclosure to unauthorised systems or personnel)				
Data Loss/Leakage Prevention (Remanence)				
Data classification and labelling				
Regulations				
Cracking				
Insecure and Proprietary APIs				
Virtualization				
Hijacking of Accounts, Services and Traffic				
Provider's Risk Profile Unknown				
Uninterrupted Availability				
Governance				
Compliance				
Cyber Forensics				
Personnel Security				
Legal issues				
Data/vendor lock-in				
Denial of service				
Malware				
Cloud bursting				

12) Kindly indicate a possible control or technique to mitigate the challenges or threats affecting the security of cloud computing data and resources.

Concern	Indicate possible control/technique applied
Data Security (Disclosure)	
Data Loss/Leakage	
Data classification and labelling	
Regulations	
Cracking	
Insecure and Proprietary APIs	
Virtualization	
Hijacking of Accounts, Services and Traffic	
Provider's Risk Profile Unknown	
Uninterrupted Availability	
Governance	
Compliance	
Cyber Forensics	
Personnel Security	
Legal issues	
Data/vendor lock-in	
Denial of service	
Malware	
Cloud bursting	

SECTION D: CLOUD DATA SECURITY

13. Does your organisation have a cloud governance policy that is followed in the implementation of the cloud?

(i) Yes [ ] (ii) No [ ]

14. a) Does the cloud service provider (CSP) adhere to any established cloud security framework(s) involving data security controls?

(i) Yes [ ] (ii) No [ ]

b) If yes, kindly name the cloud framework …….

15. Does the CSP undergo any regular (e.g. annual) 3rd party audit(s) for compliance with any established cloud security framework(s)?

(i) Yes [ ] (ii) No [ ]

16. **Data commingling** in cloud computing refers to different customers' data sitting on the same server. What technical enforcement mechanisms does a CSP use to prevent the commingling of data with other cloud users?

……..

……..

17. What mechanisms are provided for customers to define access to their data?

…….

……

18. Does the cloud service provider(CSP) offer data back-up and recovery services for customers?

Yes [ ] No [ ]

If yes, is the specific location for such selectable by the customer? …….

……

19. Does the cloud service provider(CSP) provide customers with controls over its data to ensure that data can or cannot be aggregated according to customer needs and/or restrictions?

……

……

20. Does the Cloud Service Provider (CSP) provide a capability to locate and search all of a customer's data? …….....

(i) Yes [ ] (ii) No [ ]

If yes, is this a supervised search capability or an unsupervised search capability? **.....**

21. How do you identify and evaluate service and security of cloud service providers

……

……

Data loss prevention solution is a system that is designed to detect potential data breach / data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while **in-use** (endpoint actions), **in-motion** (network traffic), and **at-rest** (data storage).

22. Does the cloud provider provide end to end encryption for

a) Data in transit (i) Yes [ ] (ii) No [ ]

b) Data at rest (i) Yes [ ] (ii) No [ ]

23. Data life cycle has six stages. They are creation, storage, sharing, usage, maintain and destroy. What are some of the security measures you apply in each stage of data life cycle?

Stage	Security Measure
Creation	
Sharing,	

Maintain	
Storage,	
Usage	
Destroy	

SECTION E: DATA SECURITY IMPLEMANTATION MODEL

24. a) in your view, does your organisation/institution require to adopt a cloud data security model?

(i) Yes [ ] (ii) No [ ]

b) If yes, state the challenges the model is expected to solve in regard to your cloud.

…….

……..

25. What areas should the cloud data security implementation model (CDSM) cover in your organisation.

Access [ ] Transit [ ] Retrieval [ ]

Storage [ ] Removal [ ] Usage [ ]

26. State the number of times when security of data in the cloud may have been breached in your organisation.

Once [ ] Twice [ ]

Thrice [ ] Many times [ ]

Kindly indicate the form of bleach …….

29. In your view which of the following cloud level/layer is most vulnerable

Kindly rate the level of vulnerability of each layer on a scale of 1 to 3 (1 = least vulnerable, 2 = moderately vulnerable and 3 = Most vulnerable)

Cloud layer/ level	1	2	3
Infrastructure			
Location			
Platform/OS			
Access			
Application			

Appendix III: Letter of Introduction

UNIVERSITY OF NAIROBI
COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES
SCHOOL OF COMPUTING AND INFORMATICS

Telephone: 4447870/4446543/4444919
Telegrams: "Varsity" Nairobi
Telefax: +254-20-4447870
Email: director-sci@uonbi.ac.ke

P. O. Box 30197
00100 GPO
Nairobi, Kenya

Our Ref: UON/CBPS/SCI/MSC(ITM)/2013

30 October 2015

To Whom It May Concern

Dear Sir/Madam

JOSEPHINE W. MUTHEE – REG NO. P54/65180/2013

The above named is a bona fide student pursuing a Master of Science in Information Technology Management degree at the School of Computing and Informatics, University of Nairobi. She is currently carrying out her research on the project entitled **"A Data Security Implementation Model for Cloud Computing in Public Institutions. A Case Study of Kenya Power and Lighting Company Ltd (KPLC)".**

We would be grateful if you could assist Ms. Muthee as she gathers data for her research. If you have any queries about the exercise please do not hesitate to contact us.

Yours sincerely

School of Computing & Informatics
University of NAIROBI
P. O. Box 30197
NAIROBI

PROF. W. OKELO-ODONGO
DIRECTOR
SCHOOL OF COMPUTING AND INFORMATICS

EOA/hmm/New D:My docs/project data collection letter