A CLOUD COMPUTING SECURITY ASSESSMENT FRAMEWORK FOR SMALL AND MEDIUM ENTERPRISES IN KENYA

SATWINDER SINGH RUPRA

A Research Thesis Submitted to the Institute of Postgraduate Studies in Partial Fulfilment for the Requirements of the Doctor of Philosophy in Information Technology Security and Audit of Kabarak University.

KABARAK UNIVERSITY

JANUARY 2020

DECLARATION

The research thesis is my own work and to the best of my knowledge it has not been presented for the award of a degree in any university or college.

Signed:

______________________________________Date: ______________________________

Satwinder Singh Rupra

GDI/M/1220/09/15

RECOMMENDATION

To the Institute of Postgraduate Studies:

This research thesis entitled "**A Cloud Computing Security Assessment Framework for Small and Medium Enterprises in Kenya**" and written by **Satwinder Singh Rupra** is presented to the Institute of Postgraduate Studies of Kabarak University. We have reviewed the research project thesis and recommend it be accepted in partial fulfilment of the requirement for award of the degree of Doctor of Philosophy in IT Security and Audit.

Signature ….. ………….. Date…02/01/2020……………

Dr Amos Omamo

Senior Lecturer – School of Computing and Informatics

Meru University

Signature … ………………………….. Date…02/01/2020……………

Dr Nickson Menza Karie

Senior Lecturer – School of Science, Engineering and Technology

Kabarak University

COPYRIGHT

ACKNOWLEDGEMENT

I would first like thank the Almighty Waheguru for giving me the strength and ability to do this research. I wish to thank Kabarak University for granting me a chance to study in the institution. I sincerely wish to thank Prof. Kefa Rabah for always having confidence in me and encouraging me to push forward. I wish to thank Dr Amos Omamo and Dr Nickson M. Karie for the time and energy devoted to this work, their invaluable analysis of the work and hope when the situation almost looked hopeless. Finally, all those who helped me in this journey, I thank you all as a PhD is not done singlehandedly but is a combination of ideas and efforts.

DEDICATION

I dedicate this thesis to my field of IT Security where my interests lie. My motivation has been my family and colleagues from the IT field.

ABSTRACT

Cloud computing plays a very important role in the development of business and competitive edge for many organisations including SMEs. Cloud computing is considered to be a very capable and able internet-based computing platform which offers numerous benefits like mobility, flexibility, reliability and cost effectiveness. Every cloud user continues to expect maximum service, and a critical aspect to this is cloud security which is one among other specific challenges hindering adoption of the cloud technologies. The absence of appropriate, standardised and self-assessing security frameworks of the cloud world for SMEs becomes an endless problem in developing countries and can expose the cloud computing model to major security risks which threaten its potential success within the country. It is further noted that security issues arise from either human error (people), lack of implementing appropriate technology or external factors like cloud providers or legislation. Security metrics can be seen as tools for providing information about the security status of a certain environment. With that in mind, this research presents a security framework for assessing security in the cloud environment based on the Goal Question Metrics methodology. The developed framework produces a security index that describes the security level accomplished by an evaluated cloud computing environment thereby providing the first line of defence. The framework was developed by first investigating the challenges faced by Small and Medium Enterprises in Kenya who use cloud computing and also by determining backend challenges in a practical manner using OwnCloud. The data was collected from the top 100 SMEs using questionnaires and further, SPSS was used to interpret the data. The data collected from the questionnaires and the experimental study were analysed through Goal Question Metrics simulation method that was used in formulating a framework on how SaaS Cloud Computing can be securely used for assessment in a SME infrastructure. This study has concluded with an eight-step framework that could be employed by SMEs to assess improved information security in the cloud. The most important feature of the developed Security framework is to devise a mechanism through which SMEs can have a path of improvement along with understanding of the current security level and defining desired state in terms of security metric value.

Keywords: *Cloud Computing, Framework, SME, Security, Standards.*

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

AWS	Amazon Web Services
COBIT	Control Objectives for Information and Related Technologies
COSO	Committee of Sponsoring Organisations
DOS	Denial of Service
DDOS	Distributed Denial of Service
ENISA	European Union Agency for Network and Information Security
EU	European Union
GQM	Goal Question Metrics
HIPAA	Health Information Portability and Accountability Act
ISACA	Information Systems Audit and Control Association
ITIL	Information Technology Infrastructure Library
PCI DSS	Payment Card Industry Data Security Standard
QOS	Quality of Service
SME	Small and Medium Enterprise / Entrepreneurship
SSL	Secure Socket Layer
TSL	Transport Layer Security
VM	Virtual Machine

OPERATIONAL DEFINITION OF TERMS

Access control list (ACL): 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 (Gartner, 2018)

Authorisation: A means by which an authenticated user is given access to secure resources controlled by the system based on their level of authority (Technology Dictionary, 2017).

Business Continuity Planning: 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, 2018).

Cloud: A set of hardware, networks, storage, services, and interfaces that enable the delivery of computing as a service (Technology Dictionary, 2017).

Cloud Bursting: 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 start up 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 centres, across multiple external data centres, or between internal and external data centres (Gartner, 2018).

Cloud Computing: Cloud computing is the provisioning of IT resources including hardware, software, or services from third parties over a network, usually the internet (Mohamed, 2009).

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, 2018).

Critical Infrastructure: Processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of citizens of a country and the effective functioning of a government (Mohamed, 2009).

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 centre to full operation after a catastrophic interruption including recovery of lost data (Gartner, 2018).

Disaster Recovery (DR) site: is a facility an organisation can use to recover and restore its technology infrastructure and operations when its primary data centre becomes unavailable (Gartner, 2018).

Distributed Computing: A model in which components are located on a network and communicate and coordinate their actions by passing messages (SANS Glossary of Security Terms, 2017)

Framework: A series of documented processes that are used to define policies and procedures around the implementation and on-going management of information security controls in an enterprise environment (Granneman, 2017)

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, 2018).

Hacker: A person gaining unauthorised access to data (Technology Dictionary, 2017).

Measured Service: Customer's use of the capabilities is monitored, controlled, reported, and charged; with complete transparency enabling a pay-as-you-use metering arrangement (NIST, 2017).

Multi-Tenancy: Enables sharing of resources and costs across a large pool of users thus allowing for centralisation of infrastructure. 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, 2018).

On-Demand Self-Service: Customers can unilaterally provision computing capabilities, without requiring human interaction with the service provider (NIST, 2017).

Paradigm: Framework that comprises the basic methodology that are recognised by members of a technical community (Granneman, 2017).

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, 2018).

Privacy: The aspect of keeping information private and secluded from third parties (SANS Glossary of Security Terms, 2017)

Private cloud: Clouds operated for the exclusive use of an organisation. Either managed by that organisation or a third party (Granneman, 2017).

Risk: The likelihood of threat to occur (Technology Dictionary, 2017).

Rapid elasticity: Near-immediate provisioning of capabilities, to quickly scale up, or down, according to demand (NIST, 2017).

Resource pooling: Physical and virtual resources are dynamically assigned and reassigned according to demand, resulting in cost savings to the customer (NIST, 2017).

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, 2018).

Secure Socket Layers (SSL): A technology for establishing an encrypted link between a web server and a browser (Granneman, 2017).

Security: The process of implementing measures and systems designed to securely protect and safeguard information against any unauthorised access, misuse, malfunction, modification, destruction, or improper disclosure, thereby preserving the value, confidentiality, integrity, availability, intended use and its ability to perform their permitted critical functions (SANS Glossary of Security Terms, 2017)

Small and Medium Enterprise (SME): A company that has a yearly turnover of between KES 70 million and 1 billion and is not listed in the stock exchange (UAE Chamber of Commerce, 2016)

Storage: Cloud storage is a means of data storage whereby the data is stored and accessed over the network, mostly through the internet (Daniel, 2014).

Unified Threat Management: 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, 2018).

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, 2018).

Virtual Machine (VM): 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, 2018).

Vulnerability: A weakness in an information system that might be exploited by an attacker (Technology Dictionary, 2017).

CHAPTER ONE
INTRODUCTION

1.1 Background to the Study

In the Kenyan market, an SME is defined by researchers as a company that has a yearly turnover of between KES 70 million and 1 billion and is not listed in the stock exchange (Adeyeye, 2016). The Nation business daily carries out a yearly survey to determine the top 100 SMEs in Kenya. Under the Micro and Small Enterprises Act of 2002, micro enterprises have a maximum annual turnover of KES 500,000 ($5,000) and employ less than 10 people. Small enterprises have between $5,000 to $50,000 annual turnovers and employ 10-49 people. Medium enterprises –while not covered by the Act have a turnover of between $ 50,000 and $ 8 million and employ 50-99 people (Kenya Gazette Supplement No. 219, 2013).

Kenya's SME is dominated by the micro and small enterprise found in city estates and along major highways. A recent National Economic Survey report by the Central Bank of Kenya (2017), SMEs constitute 98 per cent of all business in Kenya and create 30 percent of the jobs annually as well as contribute 3 percent of the GDP. Despite their immense contribution to the economy, Kenya's SMEs are faced with numerous challenges and one of the main challenges has been information technology related costs (Bowen, Morara, & Mureithi, 2009).

Business applications have always been very complicated and expensive; the amount and variety of hardware and software required to run them are overwhelming. Businesses need a whole team of experts to install, configure, test, run, secure, and update them, which most SMEs are unable to afford (Velte, Velte, Elsenpeter, & Elsenpeter, 2010). With the introduction of cloud computing for businesses, most of the SMEs are able to avoid headaches that come with storing their own data, because they are not managing hardware and software - that becomes the responsibility of cloud computing provider. The shared infrastructure means cloud computing works like a utility, where SME only pay for what they need, upgrades are automatic and scaling up or down is easy (Fox et al., 2009).

Cloud computing is a means of data storage whereby the data is stored and accessed over the network, mostly through the internet. The data is stored on multiple servers (and often locations), and the environment is controlled and managed by a hosting company called cloud storage providers (Sultan, 2010). It is a kind of outsourcing of computer programs where users are able to access software and applications from wherever they are. In other words, the computer programs are hosted by an outside party and reside in the cloud and the users do not have to worry about things such as storage and power, they simply enjoy the end result (Sultan, 2010). The providers always keep the data available and accessible wherever and whenever the owner or users require (Daniel, 2014). Put differently, cloud computing is the provisioning of IT resources including hardware, software, or services from third parties over a network, usually the internet. It is the delivery of scalable IT resources over the Internet, as opposed to hosting and operating those resources locally (Seccombe et al., 2009).

Bhardwaj, Jain and Jain (2010) assert that cloud computing is a web-service that comprises provision of storage capacity and virtualised computing resources. The virtual computing resource (email, software, data storage) are managed through remote servers by cloud providers. The cloud providers manage the cloud platform to offer their services and the end users access these services through normal browsers on computing devices such as; PC, iPad and Mobile Phones, among others (Bhardwaj et al., 2010). Therefore, end users do not have to manage or scale the IT infrastructure resources and instead focus on their core businesses. This leads to reduced running/capital costs, increased productivity, mobility, collaboration and profitability of businesses (Li, & Liu, 2011). It is a model that enables on-demand access to shared configurable computing resources which can then be configured for usage by an organisation.

These resources include applications and services, or the infrastructure on which the services operate. By deploying IT infrastructure through the cloud, an organisation can purchase additional resources on an as-required basis and avoid the initial costs of software and hardware like networks, servers, storage, application software (Buyya, Broberg, & Goscinski, 2010).

According to Kavanagh and Johnson, (2017), organisations are now comfortable to allow their employees to access their information on their mobile phones and tablets and to carry out business-critical tasks. It is clear that mobility and virtualisation has helped organisations in many industries to meet their business objectives. However, since this kind of computing paradigm is fairly new, it has shortfalls that need to be addressed to make its services more convenient to use (Vecchiola, Pandey, & Buyya, 2009).

Cloud computing is known to be very promising internet-based computing platforms, but this platform could result in a loss of security over customer data. This usually happens because the enterprise IT assets are hosted on third-party cloud computing platforms (Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009). As SMEs become more embedded in cloud computing, cyber threats on the other hand are threatening the prosperity of cloud computing in the SME sector (Sultan, 2010). The increased reliance on cloud computing and cyberspace has not only brought numerous benefits but also exposed the SMEs to a lot of cyber threats. These cyber issues range from malware that compromises with the integrity of data and privacy of critical information to denial of service (DoS) that disrupts the provision of services according to the Centre of Internet Security (2016). Whatever shapes the attack takes, the overall consequences are the same; sensitive data is at stake and the trust in the cloud goes down (Harries, & Yellowlees, 2013).

Where cloud computing can help organisations accomplish more by paying less and breaking the physical boundaries between IT infrastructure and its users, heightened security threats must be overcome in order to benefit fully from this new computing exemplar (Palmer, 2015).

The rate of cyber-attacks has increased in recent times and experts believe that if nothing is done about it, the severity of future attacks could be much greater than what has been observed currently (Cashell, Jackson, Jickling, & Webel, 2014). Cloud hackers have become innovative and have the capacity to cause harm with catastrophic impact from anywhere in the world, while equipped with only a computer and the knowledge needed to identify and exploit vulnerabilities (Reveron, 2012). It is noted that mid-sized businesses which include SMEs, focus their investment on customer satisfaction and mechanisms of reducing operating costs and therefore tend to disregard necessary investment towards securing their cloud infrastructure (Khajeh, Greenwood, Smith, & Sommerville, 2012). Therefore, they become more vulnerable than larger organisations that have dedicated budgets and personnel to handle their IT infrastructures. Cloud Computing may be offered by a vendor using three different service delivery methods:

1.1.1 Infrastructure-as-a-Service:

This cloud service model typically provides access to networking structures, computers (virtual or on dedicated hardware), and data storage space (Zhang, Cheng, & Boutaba, 2010).

Users have an allocated storage capacity and start, stop, access and configure the virtual servers and storage as desired. Cloud users may install various operating-systems and their application software on the cloud infrastructure thereafter deploying their applications (Bhardwaj et al., 2010).

In this model, the cloud users are responsible for maintaining the operating systems and the application software. Infrastructure-as-a-service (IaaS) cloud vendors typically charge their customers on a utility computing basis whereby the cost reflects the amount of resources allocated and consumed (Erl, Puttini, & Mahmood, 2013). Examples of IaaS include Microsoft Azure Amazon Web Services, Cisco Metapod and Google Compute Engine.

1.1.2 Platform-as-a-Service:

In the PaaS models, the cloud users do not control the networking structures, underlying software, hardware or servers. The cloud vendors/providers provide a computing platform, which usually includes the operating system (OS), programming-language execution environment, the database, and web server (Buyya et al., 2010). This therefore lets the application designers and developers to run their software solutions on a cloud platform without paying for expensive hardware and software layers that usually have significant costs.

PaaS removes the need for organisations to manage the underlying infrastructure and allows the cloud users to focus on the deployment and management of their applications (Armbrust et al., 2010). This increases efficiency as they don’t need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other similar background services in running your application (Hurwitz, Bloor, Kaufman, & Halper, 2010). Examples include Windows Azure, AWS Elastic Beanstalk and Apache Stratos.

1.1.3 Software-as-a-Service:

SaaS provides the cloud users with a finished product that is run and managed by the cloud vendors (Buyya et al., 2010). In the SaaS model, the consumer does not manage or control the principal cloud infrastructure including networking structures, computers (virtual or on dedicated hardware), and data storage space except the limited user-specific application configuration settings (Liu et al., 2011). Cloud users access applications through a client interface like a web browser (Armbrust et al., 2010). This is the most typical and popular model especially amongst personal uses. Examples include email, Google Apps, Zoho, I Cloud and Netflix.

The cloud computing service models and their typical uses are illustrated in Figure 1:

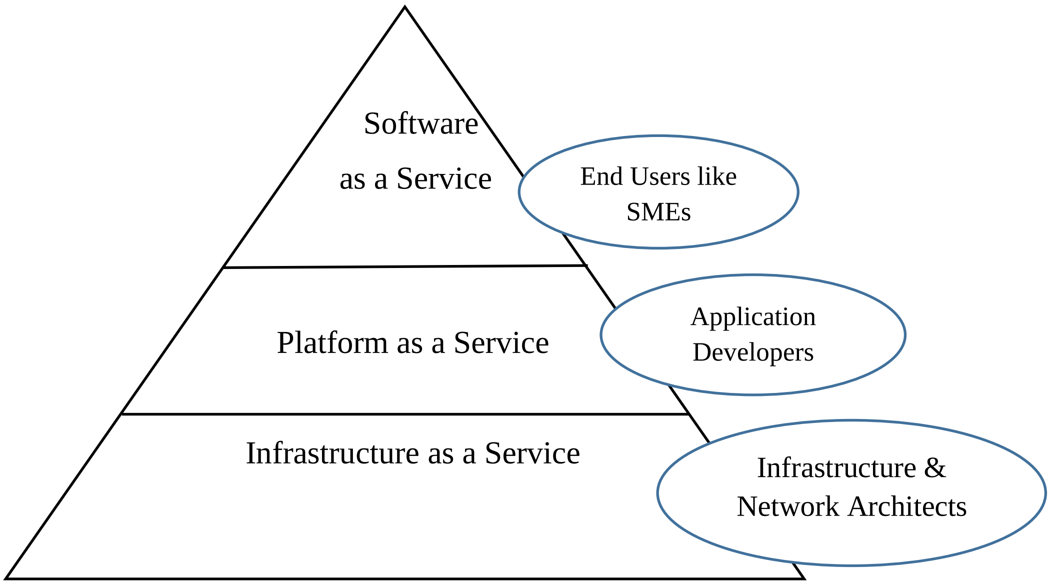


Figure 1: Cloud Computing Service Models
Source: *Author (2019)*

Cloud solutions and architecture can be deployed in four different ways as explained below (Victories, 2015):

1.1.4 Private Cloud

Private cloud setups are designed and used explicitly for private companies. The company owns all the hardware, software and resources. This type of infrastructures may be managed by the in-house IT staff or outsourced to third parties (Victories, 2015).

A private cloud is usually set up within the premises or data centre of an organisation or company but might on several occasions be stored off premises too. It is easier to align with security, compliance, and regulatory requirements, and provides more enterprise control over deployment and use but is however expensive to set up and maintain. 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. Unlike the public cloud, this type of infrastructures has all the cloud resources and applications managed by the organisation itself, similar to how the Intranet works. Utilisation on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organisation and designated stakeholders may have access to operate on a specific private cloud (Dooley, 2010).

1.1.5 Community Cloud

Community cloud infrastructure is mutually shared by several businesses, companies, society or cluster and provisions a precise group that has common goals to meet. For example, a plan, undertaking or safety requests. The cloud could be operated by the group themselves or subcontracted to experts in the market, and may be hosted from within the organisation or elsewhere (Victories, 2015).

1.1.6 Public Cloud

Public cloud setups are normally obtainable to all internet consumers or a big industry group and are owned by cloud providers who vend their services. These kinds of clouds are fairly popular for personal usage but used by smaller organisations too (Victories, 2015).

A public cloud is a model which allows companies or users access to the cloud via interfaces using web browsers or similar applications. A public cloud infrastructure is usually centred on a pay-per-use model, just like the internet bandwidth packages which are flexible enough to cater for increase in demand for internet. This helps cloud clients to better match their IT expenditure at an operational level by decreasing its capital expenditure on IT infrastructure (Hurwitz et al., 2010). Security in public clouds setup may typically not be as good as the above-mentioned cloud types. This is because they have 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 arise when dealing with public clouds with the cloud SLA at its core (Behl, 2011).

1.1.7 Hybrid Cloud

Hybrid cloud setups are a combination of two or more clouds computing infrastructures mentioned above that still exist as exclusive objects. By use of standardised or proprietary technology, these clouds are bound together and permits data and application compactness for example cloud bursting for load-balancing between clouds (Victories, 2015).

1.2 Statement of the Problem

As more SMEs today continue to use cloud computing as a vital business tool and to store their data online, the need for security of information assets of an organisation cannot be over-emphasised. SMEs are utilising the opportunities offered by cloud to adopt innovative business operations, to increase business efficiency, to develop customer-centric strategies, and to stay competitive with the use of technology. It is therefore imperative to ensure that the information stored in the cloud is protected against any kind of failures or attacks. Although, cloud computing offers several benefits for achieving business success, 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.

A baseline survey of cloud computing in Kenya in 2013 revealed that security is one among other specific challenges hindering adoption of the cloud technologies in Kenya (Omwansa, Waema, & Omwenga, 2014). Every cloud user continues to expect maximum service from the cloud, and a critical aspect to this is cloud security. The absence of appropriate, standardised and self-assessing security frameworks of the cloud world becomes an endless problem in developing countries and can expose the cloud computing model to major security risks which threaten its potential success within the country.

Currently, SMEs are facing cloud computing security issues because of the lack of customised security self-assessment framework as the existing number of standard security frameworks/guidelines like ISO 27001, Cyber Security Framework (CSF) and others, are in evolving stages for the Cloud computing environment and also do not provide methods to guide the SMEs. Apart from this, the security requirements of SMEs vary based on their specific security risks. Therefore, it is absolutely essential to have a comprehensive, end-to-end standardised security framework based on industry standards, but tailored to the specific requirements of SMEs.

1.3 Purpose of the Study

The main objective of the research was to develop a standardised cloud security framework for SMEs that would aid SMEs to self-assess and index challenges in cloud computing and therefore improving their overall security.

1.4 Research Objectives

i. To determine the fundamental cloud security challenges experienced by SMEs in Kenya.
ii. To develop a security assessment framework to address the challenges determined in the SMEs in Kenya.
iii. To propose an effective index of security in the cloud by using cloud security metrics.
iv. To test and validate the developed framework

1.5 Research Questions

i. What are the fundamental cloud security challenges experienced by SMEs in-Kenya?
ii. How can a security assessment framework that addresses the challenges determined in SMEs in Kenya be developed?
iii. Can the security in the cloud be indexed effectively by using cloud security metrics?
iv. How can the framework be tested and validated?

1.6 Justification/ Significance of the Study

The government of Kenya identified SMEs as one of the prime movers of this economy (Mwobobia, 2012). The suitability of available information security frameworks and standards for Small and Medium Business Enterprises (SMEs) is worth further investigation. According to Payne (2007), Small and Medium Enterprises (SME) play an important role in the economics of the developing countries and they are in a better situation to get the benefits of Business because: SMEs count for 60% to 70% of all employment in developing countries; SMEs adapt to the new technology faster than larger companies (less bureaucracy and stricter staffing hierarchies).

The ability of SMEs to securely use and utilise ICT in their businesses is an important prerequisite for successful business. However, many studies showed that lack of effective security is a significant barrier for the adoption of ICT infrastructure for business (Tan, Chong, Lin, & Eze, 2009; Ebrahim, & Irani, 2005). The dynamic nature of online information systems requires companies to be proactive with thwarting information security threats, and to follow a systematic way for managing and evaluating the security of their online services.

The essence of this research was first to identify the SaaS cloud security challenges confronting SMEs in Kenya and to develop a framework for safeguarding their assets so as to ensure continued optimal business operations, and to participate and compete securely in the ubiquitous cyber-market. To do this, SMEs from manufacturing, hospitality, health and finance sectors were surveyed using questionnaires and strategically interviewed on various SaaS cloud security challenges. The key factors which influence vulnerabilities were identified, including people, lack of technologies and external factors like cloud provider regulations.

1.7 Scope of the Study

This research looked at developing a framework by adopting the data security functions from Cyber-security Framework (CSF) and other security frameworks and additionally defining that cloud security threats result from people, lack of technology and external factors like cloud host. The security framework was further refined to suit cloud computing as well as SMEs by dividing the framework into metrics and sub metrics and calculating an index of cloud security. Finally, this index of cloud security can be computed using the framework showing how secure the SMEs data is while stored in the cloud.

1.8 Limitations of the Study

This study was limited by the following factors; OwnCloud (an open source version of SaaS cloud computing platform) was used to determine the backend challenges that an SME could face while using and storing data in the cloud. This was used because the researcher did not have access to the servers of enterprise cloud vendors and therefore OwnCloud was installed and hosted in a similar manner to mimic enterprise clouds and determine these challenges.

Data collected consisted of self-reports by directors or CEOs, finance in charge, IT administrators and data/system users filled in the questionnaire, the responses may or may not correspond to their unique facts as it is in their organisation. Some of the respondents might have lied to depict their organisation in good light. There is also danger of respondents not answering the questions honestly for fear of revealing secrets of their organisations as regards to storage of data in the cloud. To minimise this problem, respondents were assured of confidentiality and that only aggregate data would be reported.

The study was conducted on selected SMEs in Nairobi, Kisumu and Mombasa to represent the entire SME cloud users of Kenya. This is because of the fact that they exhibit the major share of SMEs that utilise IT resources for infrastructure growth and because the cities are well connected in terms of internet. However, the study attempted to utilise appropriate sampling techniques and procedures to obtain required sample size that generated the least marginal errors.

1.9 Assumptions of the Study

The study was based on the following assumptions

i. That all participants responded accurately and honestly regarding their cloud computing security.

ii. That the selected sample for the study was a representative of the population to which references were made.

iii. That the scales used for data collection yielded valid and reliable information for answering the research objectives and questions.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

This chapter started by outlining the properties and advantages of cloud computing as well as describing its importance for the SMEs in detail. The chapter further highlights the cloud computing security challenges, threats and risks as related to SMEs. Further to this, other frameworks are discussed highlighting their strengths and shortcomings and similar studies in the same field are also reviewed. To sum up the chapter, the conceptual framework was formulated showing how the variables interlink with each other.

2.2 Properties of Cloud Computing

The National Institute of Standards and Technology defines cloud computing as “a model for aiding suitable, access to a shared pool of IT assets, on-demand and through the network. These resources can be swiftly assigned and unassigned with little administration or cloud provider intervention”. However instead of these mentioned resources being accessed through the file explorer or network drives, they are accessible through a web browser like Internet Explorer or application software (Mell, & Grance, 2011).

Cloud computing and cloud have been defined in many different contexts by different sources, however cloud computing may be summarised as a fairly recent business model that delivers computing services through the internet in an expandable, flexible and anytime accessible manner (Williams, 2010). Cloud computing is viewed as a promising technology in the computing world that is supposed to provide the convenience of data accessibly at any time and any place provided one has an internet connection. Cloud computing in its simplest form can be visualised in terms of email. Anything stored on email platforms like Gmail, Yahoo, and Hotmail among others is a clear example of the cloud computing paradigm (Williams, 2010). Putting this into context make us realise that cloud is indeed being used by almost all users of the internet. Dash, Saini, Panda and Mishra (2014) indicated that for a paradigm to be classified as cloud computing, it usually possesses the following characteristics:

i. **Elasticity**: Cloud users can at their convenience downsize/upsize computing resources, as and when need arises, without human interaction. This means that to add or reduce resources on the cloud, one will not need to buy additional hardware, users can do this by the use of controlled software (Erl et al., 2013).

ii. **Access on multiple devices**: Users of the cloud are not limited to the number or type of devices they use. Mostly, if devices can access internet and have the relevant cloud applications, a user can connect to the cloud from any device (Williams, 2010).

iii. **Accessible anywhere**: Cloud customers may be able to access their data and service irrespective of the geographical location. Therefore, the cloud user has no control or whereabouts of the location of the assets. Similarly, the cloud vendor does not have restrictions over the location of its users. (Wahlgren, & Kowalski, 2013).

iv. **Reliability**: Clouds are usually backed up on multiple redundant sites sometimes even offshore, therefore all data saved on the cloud has disaster recovery catered for (Delettre, Boudaoud, & Riveill, 2011).

v. **Financial prudence and price value:** Irrespective of the cloud type, the cloud setups tend to be as large as possible in order to benefit from financial prudence. Therefore, cloud vendors can be located in areas where electricity and real estate prices are lower eventually lowering their start-up and running costs (Erl et al., 2013).

2.3 Benefits of Cloud Computing

The shift from grid computing to cloud computing is getting more evident by the day. Cloud computing offers numerous benefits which could not be attained in the native computing infrastructure (Rittinghouse, & Ransome, 2016). The advantages of using cloud computing include the following:

i. **Mobility**: The primary benefit of cloud computing by far would be the ability to access data from anywhere at any time. Once cloud users have registered themselves to a cloud vendor, all that is needed is an internet connection to be able to access their information and services. This feature lets users move beyond time zone and geographical boundary issues (Williams, 2010).

ii. **Flexibility**: Users only have to pay for services and capacity which they are really using. So, if they need less, they pay less and if they need more, they can simply acquire additional storage and services, which of course leads to higher costs, but it is still much more flexible than adding another server to the company internal IT resources. The addition or removal of processing units or storage space does only take seconds to minutes and not days like it would in a company internal data centre using physical servers (Granneman, 2017).

iii. **Reliability**: Cloud computing also adds to reliability of data in case the user loses their device. If a laptop or mobile phone is stolen, the user’s data cannot be lost since it is stored in the cloud; the user can simply buy another device and connect it to the internet to access their data (Erl et al., 2013).

iv. **Reduction of cost**: Many cloud services are provided for free and offer enough functionality for most of the users. Therefore, users can save much money by using cloud services (Jansen, 2011).

v. **Allow IT people to concentrate on other areas** by taking the load of data storage, application control and update from off their work (Williams, 2010).

2.4 Cloud Computing Paradigm for SMEs

Developing economies have embraced the emergence of ICT technologies to promote their development agenda and to present new opportunities for economic empowerment of its citizenry. In a forum organised by International Telecommunications Union (ITU) in December 2011, the speakers stressed on the need for developing economies to be aware and prepared about cyber-security risks. According to ITU, developing economies usually have peculiar challenges for their ICT requirements, requiring customised solutions.

2.4.1 SMEs and their Significance

In the Kenyan market, an SME is defined as a company that has a yearly turnover of between KES 70 million and 1 billion and is not listed in the stock exchange. Small and medium-sized enterprises (SMEs) consist of many different kinds of businesses usually operating in the service, trade, agri-business, and micro-finance and manufacturing sectors (Letting, & Muthoni, 2013). SMEs may be innovative and entrepreneurial, and usually aspire to grow; though, some stagnate and remain family owned.

SMEs are often classified by the number of employees, annual revenue and/or the value of their assets. Julien (1998) formulated some concepts of SMEs such as the firm being small in size in comparison to large or multi-national corporations; they are said to be characterised by the following: Having centralised management; having a low level of labour specialisation; having simple, informal and direct internal and external information systems; having intuitive, implicit and short-term strategy.

SMEs are one of the principal driving forces in economic development. They help to diversify economic activity and make significant contributions to the economy. They are crucial to most countries’ economic stability and constitute the majority of businesses, accounting for over 50% of employment (Ongori, & Migiro, 2010).

Different studies reveal that there are several opportunities that technology and the internet provide for SMEs in developing countries (Hooks, & Duncombe, 2001; Parker, & Castleman, 2007). Information systems projects in developing economies are characterised by socio-economic changes or transformations, as they seek knowledge and skillset to the SMEs. Walsham and Sahay (2005), examined various literatures on information systems research in developing economies, and underscored their relevance. The emergence of Internet facilities in developing economies have impacted positively on societies and organisations, especially in areas of connection costs, access speeds and end-user’s utilisation (Ellefsen, & Solms, 2012).

Ellefsen and Solms (2012) reasoned that developing economies are usually overwhelmed by the massive and rapid improvements of the emerging technologies in ICTs. For instance, most SMEs do not have any programs in place to harness the increased bandwidth, with its attendant vulnerability challenges confronting their systems and their customers. SMEs in developing economies are said to have unique challenges, and therefore direct importation of existing ICT solutions from the developed economies may not necessarily address the issues effectively.

2.4.2 SMEs and Cloud Security Challenges.

The idea behind cloud computing from an SME’s point of view is that instead of having the software and data stored locally on servers within their premises, they can all be stored on Internet servers, “in the clouds,” and accessed as a service on the Internet. As a consequence, users do not have to worry about storage capacity, memory, endless hardware purchases and upgrades (Lanois, 2010).

The adoption and implementation of cloud solutions has been on the increase with many SMEs in developing countries adopting the cloud computing offerings. For SMEs without adequate computing resources this is a viable solution and is facilitated by existence of cloud service providers who provide cloud services for free or at discounted rates to educational institutions (Mokhtar, Al-Sharafi, & Aborujilah, 2013).

Compared to large businesses, SMEs have been slow in adopting technological innovations. Large firms can take greater risks associated with innovation adoption, because they have more resources and greater economies of scale (Kuan, & Chau, 2001). It is critical for SMEs to benefit from new information systems and technologies because SMEs constitute the large majority of all business in many developing economies including Kenya. The large number of SMEs reveals their importance as an essential source of jobs.

Cyber-security vulnerabilities pose serious concerns to all businesses however SMEs are usually hardest hit victims and find it very difficult to recover after a cyber-attack (Boateng, 2013). SMEs are easier targets than large corporations. Large corporations have, in recent times, strengthened their security systems, either as a response to the increased threats or in compliance with regulations.

Besides the positive aspects of technological adaption, employees often refuse to adopt new technologies because of the perceived danger of job loss or unwillingness to change their working practices. As a consequence, SME owners are often reluctant to bring their business through a learning curve which proves to be difficult, disruptive and costly (Chian, 2010).

Organisations support the introduction of innovations when the existing process or service is replaced with one expected to be an improvement over the current system (Gallivan, 2001). Additionally, firms may seek innovations due to pressures associated with maintaining a competitive advantage or gaining recognition within an industry.

Many SMEs do not consider themselves as having data that is of interest to cyber-criminals and quite often dismiss the need for properly addressing vulnerabilities in their infrastructure. Pierre (2008) states that the opposite is in fact true; every business today collects data on employees, customers and vendors that are of interest to cyber-criminals.

2.5 Challenges in the Cloud

Cloud computing is not a standalone computing platform, it instead combines several technologies. These include networks, operating systems (OS), databases, virtual servers and components, resource scheduling, transaction processing, concurrency control techniques, load balancing, memory management and numerous others for its functionality and operation (Shroff, 2010). Therefore, a threat in any one of the technologies becomes a threat for the entire cloud platform. Most security problems stem from loss of control, lack of trust or multi-tenancy. These problems are described below in more detail:

2.5.1 Loss of control:

Since most cloud platforms are hosted off-site, an organisation cannot have full control over the hardware, technology and backend details of the cloud platform. Usually, when an organisation outsources their data and services to a cloud vendor, they are not aware and have no control over the location of their data. This possesses serious concerns from a user perspective; organisations lose control over their vital data and are not aware of any security mechanisms put in place by the provider (Behl, 2011). According to Tech Target, having data in an unknown place and with no control over it is one of the leading concerns to organisations when switching to cloud computing.

According to Pearson and Benameur (2010), user-centric control does not seem like a possibility with the cloud: as soon as a SaaS cloud infrastructure is used, the cloud vendor becomes responsible for storage of data, loosing visibility and control over it. In the cloud paradigm, users' data is processed in 'the cloud' on hardware, software and platform they do not own or control, and therefore becomes a threat in terms of theft, misuse (especially for different purposes from those originally notified to and agreed with the consumer) or unauthorised resale.

Additionally, it is not clear that it will be possible for a cloud provider to ensure that a data owner can get access to all their data including metadata and system related files. Furthermore, there is no sure way of telling that documents or personal data on the cloud has been successfully deleted if the user wants to. Some vendors may also deliberately tie down a customer to proprietary software or hardware so that it becomes difficult to switch providers (Behl, 2011).

As an example, consider a company X in Nairobi that is using a cloud provider Y who stores their data in India and Australia. X's data is stored on Y's cloud and therefore is transmitted between various hardware and software devices located in the three locations. These additional links require X to entrust its data to different systems and platforms located in different locations, managed by unknown users, and regulated by the laws of other countries (India and Australia).

In such a scenario, X does not know whether the security profiles of the remote locations are the same as what they have in-house or whether the regulatory compliances like HIPAA hold in all the locations. X will realise that as soon as the data leaves their perimeter in Nairobi, it does not have much control over it or what processes it goes through. X does not know who can access its data that is now stored on various disks in multiple locations (India and Australia). This lack of control over the data and processes by X triggers the risk of losing data confidentiality, integrity, and availability (Khan, & Malluhi, 2010).

Cloud computing essentially requires a customer to hand over any control of running their applications and storing their data to their providers. They retain only partial control of their data, which is a cause of concern for them. A consumer relies on their provider to ensure data security and privacy, resource availability, monitoring and repairing of services/resources. Therefore, it goes without saying that the consumer has to be sure of what the cloud provider is doing in terms of security.

2.5.2 Lack of Trust

Trust can be defined as an act of faith, confidence and reliance in something that one expects to behave as stated. It is a confidence in the ability and expertise of others, such that one feels they can rely on an entity to care for your valuable assets. Trust in a system is reduced when we have little or insufficient information about its expertise (Khan, & Malluhi, 2010).

Trust also has a variation depending on the data ownership. For example, if a company stores and executes their data on the cloud, it creates two folds of a trust relationship (Velte et al., 2010). Primarily, the company must trust their cloud provider and secondly, the company must make sure that its clients also trust the same provider. A provider and customer often enter into a contractual relationship to establish trust. Typically, a company may be compensated in an event that the service is not delivered as expected and in the case of cloud providers service-level agreements (SLAs) can be used to boost trust. However, in the modern computing world, establishing trust in cloud computing is related to preventing a trust violation rather than to compensate a violation in case it occurs. For any modern organisation, a security breach irreparable and money or compensation cannot bring back lost data or the organisation’s reputation.

Therefore, cloud computing trust model should focus more on preventing security breaches as opposed to post-failure compensation (Khan, & Malluhi, 2010). Another vital constituent of cloud trust is reputation, which is arguably a provider's most valuable quality.

A consumer's insight mostly is that cloud computing is not as secure as internal paradigms; however improved transparency can counter this. Data stored in cloud devices is stored and processed across the entire virtual layer. Two issues arise from this in relation to trust: firstly, the physical storage and processing sites are unknown to the data owner, and secondly the security implementations in these sites. A company should know where its data is processed and stored, because laws in different countries may not be favourable to the company in case of breaches. A company also needs to know how its data is protected while being moved within the system or across multiple sites owned by the cloud providers (Khan, & Malluhi, 2010). If there is no transparency between the provider and the customer, a company will not know if their security requirements are in line with the cloud provider's security assurances.

Ultimately, usage of the cloud is a question of trade-offs between security, privacy, compliance, costs, and benefits (Pearson, 2013). Trust is a vital component to the adoption of cloud computing and therefore trust needs to be included right along the chain of service provision.

2.5.3 Multi-tenancy issues:

Multi-tenancy is one of the properties of cloud computing that depicts resource sharing. Numerous resources are shared comprising of the processing, applications, networks and information. Cloud computing heavily relies on an operational model where resources are shared. This means that more than one user to use the same resource at different levels including the network, host and application. The cloud users utilise the same hardware despite being isolated at a virtual level, thus an attacker can legitimately be in the same physical machine as the target. The concept of multi-tenancy is similar to the concept of multitasking in operating systems (Velte et al., 2010).

Multi-tenancy in cloud computing is unique such that both the attacker and the victim are sharing the same physical hardware like servers. A setup like this cannot be countered by native security measures and controls. This is because they are not designed to secure inside the servers and they are limited just to the network layer (Khalil, Khreishah, & Azeem, 2014).

According to Saripalli and Walters (2010), by spending a little money to buy cloud space, an attacker has a 40% chance to allocate his VM next to the victim’s VM. After such a multi-tenancy has been achieved, any attack takes advantage of the system characteristics can be launched to hack breach the victim’s data. The risk from for such an attack (like side channel attacks) is high because they cannot be detected by the hypervisor or the operating system.

Cloud computing also faces additional set of challenges as described below:

i. **Downtime**: This is a major disadvantage of cloud computing especially in evolving countries. Many parts of Kenya still face challenges with stable and affordable internet connections. Because all the data, resources and applications are only accessible through the internet, an internet outage means users have no access to them. Downtime may be reduced by having multiple ISP connections in an organisation; however, that also means an increase in cost (Williams, 2010).

ii. **Privacy Challenges**: Privacy risks always exist on data and information stored online. Like all data stored online, data on the cloud is prone to accidental leakage or compromise (Sallé, 2004).

iii. **Security Challenges**: This is the biggest question that arises to the managements of any organisation that wants to move to the cloud. Since cloud is a collection of different technologies and fields, security issues for each of these technologies becomes a threat to the cloud too. For example, networks and databases have their security threats like man in the middle attack or SQL injection attacks, which become threats to data in the cloud too (Rouse, 2014).

    Threats and flaws in other technologies like operating systems, virtual platforms, transaction processing systems, concurrency control procedures and the likes also form part of the cloud security issues. It is therefore also of utmost importance that each of these cloud technologies be secure enough to provide for overall security of the system. For example, the network between the end users and the cloud infrastructure needs to be secure (Ionescu, & Tudoran, 2013).

Data at rest also needs to be secure by encrypting the data and enforcing relevant policies for data sharing. Additionally, resource distribution and memory management systems need to be secured. Lastly, methods for malware detection also need to be employed in the clouds similar to the approach commonly implemented in intrusion detection systems (IDSs) (Sen, & Sengupta, 2005).

2.6 Security Threats for IS on the Cloud

In the modern era of technology including cloud computing, information security has become a critical business enabler as opposed to convectional processing and technology. With the new and evolving tools, standards, frameworks and technologies available and evolving, SMEs have pretty decent to average way of aiding them to secure their operations, critical information and hardware and software infrastructure. Despite this, SMEs still have challenges to keep up with regulatory requirements, economic conditions and risk management (Sultan, 2011).

Many organisations are yet to clearly understand the role of information security in their operations. Many bosses and senior management especially in small or medium organisations feel that information security is just an additional cost that they occur, however on the contrary, effectively managed information security organisations can be instrumental in helping an enterprise meet its business goals by improving efficiency and aligning business objectives (Sallé, 2004).

Small organisations may time and again interpret information security in isolation: often thinking that security is not the organisation’s responsibility and on the contrary is someone else’s responsibility. Therefore, there senior management and staff make little effort to link the security implementations and aspects to business goals. As a result of this tagged approach, it is quite easy to suffer weaknesses in security management, and could result in to serious exposure. From a financial perspective, it is quite possible for this lack of understanding to result in unnecessary expenditure on security and control as security is tacked after a breach occurs instead of prevention (Wheeler, 2011). From an operational perspective, information security efforts might not be able to achieve the intended business benefit, which may also result in information at risk.

Some SMEs might interpret information security as being just a technical aspect. Although information technology offers implements that are vital for protecting information, information technology in itself is not an acceptable solution. To prevent breaches and safeguard information, SMEs need to establish information security policies that are supported by standards, procedures and frameworks (Veiga, & Eloff, 2007). The guidance establishes the direction for the information security program and expectations as to how information is to be used, shared, transmitted and destroyed (Whitman, & Mattord, 2011).

In many enterprises, technology strategies, policy, process and standards are developed without an understanding of how organisational culture impacts program effectiveness. Security efforts that fail to consider how humans react to and use technology often do not deliver intended benefits. Information security programs need to take into account how the organisation and its people, processes and technologies interact, and how organisational governance, culture, human factors and architectures support or hinder the ability of the enterprise to protect information and to manage risk.

Information security managers have struggled to create programs that are aligned with enterprise goals and priorities, that bring value to the enterprise, and that support the ability of management to innovate while controlling risks (Veiga & Eloff, 2007). Developing an information security program and integrating it into business goals, objectives, strategies and activities are complicated by the lack of a model that describes what an effective information security program encompasses, how it functions, and how it relates to the enterprise and the enterprise’s priorities (Ionescu, & Tudoran, 2013). What is missing is a descriptive model that business unit managers and their counterparts in information security can use to talk about information security in business, rather than technical, terms (Rouse, 2014).

Securing any information system includes firstly identifying the unique threats and challenges that pertain to the system and thereafter implementing the relevant countermeasures to be overcome the threats and reduce the security risks (Longley, Shain, & Caelli, 1992). Eventually, the identified security requirements and selected security measures are introduced to the development and integration process, to incorporate the security controls with the information systems requirements. These include both functional and operational requirements, and may include other related system requirements like reliability, maintainability and supportability (Zardari, & Bahsoon, 2011).

Cloud computing paradigm includes numerous security benefits due to the nature of its technology. These include centralisation of security, redundancy and high availability. Although much of the traditional challenges posed by security threats are countered effectively due to the infrastructures of the cloud, several peculiar security challenges are introduced. Cloud computing may require risk assessment in aspects like availability and reliability issues, data integrity, recovery, and privacy and auditing (Ionescu, & Tudoran, 2013).

Security in general for any system, is usually related to confidentiality, integrity and availability; these therefore are vital components when implementing any IT system securely (Rouse, 2014). The aspects of security discussed above apply to the three broad categories of assets which need mandatory securing. These are data, software and hardware resources. The importance of confidentiality, integrity and availability in the cloud paradigm is discussed in detail in the below sections.

2.6.1 Confidentiality

Confidentiality is one of the pillars of CIA that simply means protection of information from unauthorised disclosure. This means that only authorised personnel have the ability to access protected data. Since the cloud has numerous points of access due to the devices and applications involved, threats of data breach increase in the cloud platform. Although virtually the users are isolated, the underlying hardware is usually one and the same. This can cause problems with data confidentiality if not implemented well (Zissis, & Lekkas, 2012).

Confidentiality can further be breached accidentally due to data remanence (Tim, Subra, & Shahed, 2009). Due to a nominal erase or remove operation, some data residue may be left intact. This may lead to the unwilling disclosure of private data to a user that may have purchased a big storage space and then search it for sensitive data.

Confidentiality in the cloud is associated with user authentication. Authentication is a method of creating confidence in user identities, which is presented to an IS by electronic means. If proper authentication procedures are not used, a breach in privacy could occur by users gaining unauthorised access (Zissis, & Lekkas, 2012).

Confidentiality in a software system is as equally important as data confidentiality for the overall security to prosper. In a cloud environment the user is obliged to outsource “trust” to software provided by the cloud provider. Software applications or interfaces that interact with the user’s data must be curtained not to pose any additional threats and risks. Unauthorised access may take place due to an application vulnerability or weak identification, increasing chances of confidentiality and privacy breaches (Modi et al., 2013). Additionally, the cloud provider should provide secure cloud instances that ensure users privacy.

2.6.2 Integrity

The second aspect of IS security is integrity. This means that all information (and sometimes hardware and software) should only be amended or edited by personnel who have the authority to do so. Data Integrity refers to securing data from unauthorised changes including deleting or modification (Sun, Zhang, Xiong, & Zhu, 2014). By denying unauthorised access, a customer can achieve better assurance and integrity in data. Furthermore, this can also offer greater accountability on whom or what may have altered data or system information. Authorisation is a means by which an authenticated user is given access to secure resources controlled by the system based on their level of authority (Zissis, & Lekkas, 2012). Because the cloud allows may access points for its users to connect (usually from anywhere with internet access), authorisation is crucial to maintain data integrity and security at large.

A cloud computing provider is entrusted by their clients to provide integrity for their data. However, due to the working nature of the cloud model, several threats including sophisticated insider attacks can take place. Data can be deleted, modified or changed purposefully or accidentally. For example, an unhappy employee may purposefully fabricate a program to fail when a certain command is executed or a certain time is reached. Additionally, the security of cloud services is dependent on the security of the API or interfaces that the cloud providers offer to their customers. If unauthorised users gain control of them, data integrity can be seriously violated (Stallings, & Brown, 2008). Cloud providers may need to also address hardware and network integrity, as they control the entire hardware and network resources in a cloud model.

2.6.3 Availability

Availability is an attribute of information security that means that a system is always accessible and usable whenever requested by an authorised entity (Zissis, & Lekkas, 2012).

System availability includes the ability to carry on operations even when parts of the system fail or malfunction. A secure system must be able to continue operating even if a security breach occurs. A cloud provider needs to assure that all the relevant aspects of the cloud are available to clients upon demand (Takabi, Joshi, & Ahn, 2010).

2.7 Security Analysis of Cloud Computing by Various Bodies

Different recognised security bodies have analysed areas of concerns on cloud computing and have explained how threats in the cloud affect data. This is discussed as follows:

2.7.1 Trusted Computing Group

As shown in the Figure 2, there are six crucial areas in the cloud that require protection to be able to suffice against the threats (Trusted Computing, 2010). These areas are discussed below:

i. Security of data at rest – This means data should be secure when it is stored in the cloud server(s). This is usually achieved by providing encryption for all data stored.

ii. Security of data in transit – Means that data should be secure when being transferred from the cloud to the user computers and vice versa. This can be achieved by providing TLS/SSL security.

iii. Authentication of users – Users who have access to data should pass some sort of access control to be able to keep off unwanted users. These include strong passwords and biometrics among others.

iv. Robust isolation between data belonging to different customers – Although not applicable to private clouds, however for public clouds each customers data is isolated using different VMs.

v. Cloud legal/regulatory issues – All customers should usually have their legal and regulatory experts inspect cloud provider policies and practices especially for things like data retention, deletion and security.

vi. Incident response – Customers should understand how incidents and disasters will affect their data and should therefore implement relevant recovery procedures for the same.

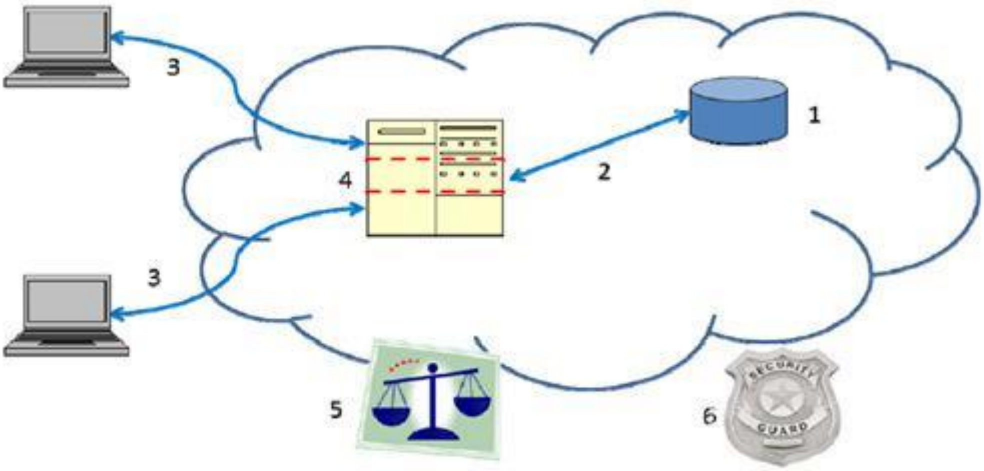


Figure 2: Areas of concern in cloud security
Source: *Trusted Computing Group's White Paper (2010)*

Cloud computing is a fairly recent technology in comparison to other technologies in the computing timeline. Therefore, there are not many common and industry accepted cloud security standards, posing additional challenges for users and companies (Mather, Kumaraswamy, & Latif, 2009). Usually, cloud vendors come up with different technologies and standards to increase their security; however, ultimately it is the responsibility of the client to ensure that security in the cloud meets their internal security standards and requirements. This could be done by carrying out risk assessments and due diligence of the cloud security models (CPNI Security Briefing, 2010).

It can clearly be noticed that cloud security threats are not substantially different from the native computing security threats. Many of the security threats and challenges in cloud computing will be familiar to organisations managing in house infrastructure and those involved in traditional outsourcing models (Mather et al., 2009). Most cloud computing threats are a consequence of attackers that can be divided into two distinct categories:

i. An internal attacker – This is usually an employee of the cloud vendor, the cloud customer or other third-party provider organisation supporting the operation of a cloud service. They may have existing authorised access to cloud services and customer data or supporting infrastructure and applications (Jansen, 2011). Internal attackers may use existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within the cloud service (Sen, 2013).

ii. An external attacker – is one that is not employed by any of the parties involved in the operation of the cloud paradigm and do not have any legal access to the data and processes in the cloud (Keller, Szefer, Rexford & Lee, 2010). External attackers exploit technical, operational, process and social engineering vulnerabilities to attack a cloud service provider, customer or third-party supporting organisation. They then gain further access to propagate attacks against the confidentiality, integrity and availability of information within the cloud service (Sen, 2013). They are more commonly known as hackers.

2.7.2 ENISA Top Security Risks with Cloud Architecture

According to Cloud Risk Assessment report published by ENISA in 2009, the following cloud specific risks have been identified:

i. **Loss of Control**: When using the cloud infrastructure, the clients usually gives away control on several issues that could affect security. In such a case, the security services are usually not committed and documented in the SLAs therefore leaving a gap in the security defences. The cloud vendor also usually does not allow the client to carry out audits and this also means that certain kind of compliances cannot be achieved. For example, PCI DSS. This has been earlier discussed in more details.

ii. **Management interface compromise**: Most management interfaces in the cloud platform are accessible through the internet browsers. These interfaces are connected to a larger set of resources and therefore pose an increased risk especially through web browser vulnerabilities.

iii. **Data protection**: Cloud computing poses a number of data protection risks. Because the owner of the data has not control over the data handling practises of the cloud vendor, there is no sure way of telling that data is being handled in a lawful way.

iv. **Insecure or incomplete deletion of data**: Whenever the data owner makes a command to delete a cloud resource, there is not certain way of telling that the data has been deleted to its entirety. This could possibly be because either extra copies of data are stored for backup purposes and therefore not available to the client or because the disk shares data from other clients and hence cannot be destroyed.

v. **Malicious insider**: A cloud administrator may become a very high risk if turn rouge and try and access data stored on clouds. Although this is usually less likely, the potential damage that may be caused by malicious insiders is often far greater.

vi. **Availability Chain**: The internet connectivity forms a single point of failure as far as the cloud is concerned. This means that if the internet is down, then there is no cloud access and therefore loss of availability.

The risks discussed in the section above are not based in a specific order of criticality; in terms of criticality, loss of control is considered as the top potential risk when working in a cloud environment. The risks of using Cloud computing should be compared to the risks of staying with traditional solutions, such as desktop-based models. (Reveron, 2012).

2.7.3 Cloud Computing and Information Policy Group

According to Jaeger, Lin and Grimes (2008), at a minimum, users will expect that a secure cloud will provide the following:

i. **Reliability and Liability**. SMEs and any businesses will expect the cloud to be reliable, when the cloud provider takes control over critical applications and data, they will expect proper description and account of liability in case of any problems (Mohamed, 2009).

ii. **Security, privacy, and anonymity**. SMEs and businesses will expect that the cloud provider will cater for confidentiality, integrity, availability and sensitive data will remain private. Extra caution has to be taken to safeguard the users' data as well as the applications for managing the data (Mathisen, 2011).

iii. **Access and usage restrictions**. SMEs and businesses alike will expect to have access to their data whenever they require and from wherever they require without any interruption from the cloud provider or any other involved parties. At the same time, their intellectual property rights should not be infringed (Khan, & Malluhi, 2010).

2.8 Cloud Computing Trends in Africa and Kenya

Cloud Computing is a fast growing trend in Africa although there is lack of cloud computing awareness in many key organisations (Gartner, 2018). According to a Gartner (2018), half the respondents in emerging markets either had not heard of Cloud Computing or did not know what it meant.

In Kenya, cloud demands are high in the offshoring industry and technology hubs. In South Africa, the call centre industry has been a fastest growing area for cloud-based technology (Akhusama, & Moturi, 2016).

2.8.1 Cisco and World Wide Worx Study

A study conducted by Cisco and World Wide Worx called Cloud in Africa: Reality Check 2013 suggests that South Africa, Kenya and Nigeria are leading countries in use of cloud computing in Africa as at the time of publishing. Further according to this study, as of 2014, 24% of organisations in Kenya had claimed that they will start using the cloud in the coming year however this did not happen because organisations are still confused about the technology.

2.8.2 International Telecommunications Union (ITU) 2012 Study

According to a study conducted by International Telecommunications Union (ITU) in 2012 in Rwanda, African countries have introduced cloud computing at different levels. There are many initiatives by individual countries to upgrade and revise legislative and regulatory frameworks. The conclusions drawn from the study are summarised as below:

i. The main characteristics of cloud computing, i.e. economies of scale (sharing) and flexibility/modularity of use, constitute opportunities for ICT development in Africa. However, these same characteristics, which translate into a very high concentration of resources and data in data centers and free public access, give rise to technical and legal situations that are highly complex.

ii. Even so, given the associated cost reductions and flexibility, the migration to cloud computing is attracting many African users.

iii. However, the absence of appropriate regulatory frameworks and lack of adequate competencies in Africa can expose the cloud computing model to major security risks which threaten its potential success within the continent. The survey conducted within the framework of this study reveals that major concerns associated with data confidentiality, data protection and network reliability have yet to be dispelled.

iv. The introduction of strategies aimed at upgrading legislative and regulatory frameworks and the launch of capacity-building programmes are strongly advocated in the interests of enabling African countries to rise to the challenge of a successful migration to cloud computing while maintaining conformity with international standards and with best practices in that sphere, thereby smoothing the way for Africa's integration into the worldwide digital economy.

As of 2012, all countries surveyed indicated that cloud computing was being considered in the country. The study targeted all South Sahara African countries. Twenty-five countries were surveyed. The study revealed that in 68% of the countries surveyed, the government administration was at the stage of studying the introduction of cloud computing. 11% were piloting, 16% implementing while 5% were already using.

At the level of the mobile operators, cloud computing technology was already used by 33% of the African country operators surveyed, while 23% of those operators had embarked upon its implementation. In the study, over 50% of the economic operators such as big companies had already adopted cloud computing.

2.8.3 Microsoft and University of Nairobi Study

This study conducted by Microsoft Kenya and University of Nairobi in 2014 describes that despite cloud service being available by many national and international providers, not many users have been keen on adopting it and are generally waiting for the feedback of everyone else. The study found out that 70 per cent of the organisations sampled were using some form of cloud services and most users have started using the services in either 2010 or 2011. The acceptance of cloud computing is however quite slow due to inadequate government policies which makes the users cautious and doubtful.

According to ICT Authority, these challenges will remain unless users are made more at ease about their data. Most users are concerned with the confidentiality, integrity and availability of their data and until cloud providers can assure this, the adoption will remain slow.

Additionally, many companies using shared data or public clouds want to have systems where they can authenticate who accessed and/or modified the data, and at what time. This will increase the integrity of their data. The study, which was the first of its kind in the country on cloud computing, was carried out in 60 organisations, with 54 respondents taking part.

2.8.4 Summary of Cloud Usage in Kenya

The cloud services as seen for the three studies is set to increase however there is lack of awareness and also fear on how secure and effective cloud is in terms of confidentiality, integrity and availability. The paradigm is used to a basic extent like simple email services and personal data storage like Dropbox, Google drive and Microsoft One drive. Enterprises and corporates have not picked up the trend with cloud computing as they should. Microsoft has been offering cloud computing services in Kenya for some time, but their frustration has been the fact that people don't understand what cloud is about. Most people who essentially should be using cloud don't, because they don't understand what it is (Kachwanya, 2011).

2.9 Cloud Security, Risk, Threats and Vulnerabilities

The body of knowledge on subjects related to cloud computing vulnerabilities, threats and risk is very large and growing. This research considered more than 200 personnel primarily from different areas working within SMEs. The result is a review that details a broad range of cloud computing challenges that confront SMEs in Kenya. These include personnel security due to improper training, cloud availability issues, cloud policy issues, improper data deletion in the cloud among others. Cyber incidents, whether caused by intentional or unintentional entities or processes are immaterial as far as the impact is concerned. Rather the ability to identify the threat agents and to understand the vulnerabilities, and take appropriate steps to mitigate the risks is of paramount importance (Romanosky, 2016).

The International Telecommunications Union (ITU) identifies eight (8) data and information security dimensions; namely, authorisation, authentication, availability, communications security, confidentiality, integrity, non-repudiation and privacy. Several other experts have attempted to propose alternative information security properties. For example, Dhillon and Backhouse (2000) develop the CIA triad with their RITE security principles of responsibility, integrity, trust and ethicality. Parker (2012) proposes six (6) cyber-security attributes of control, authentication, utility, confidentiality, integrity and availability. However, universally, the classical cyber-security triad of confidentiality, integrity and availability (CIA) has become the foundation of most information and data security assessment. This research thus focuses on achieving security in the cloud as defined in the CIA triad shown in

Figure 3. The CIA triad has been explained in details in section 2.5 of this research.

`

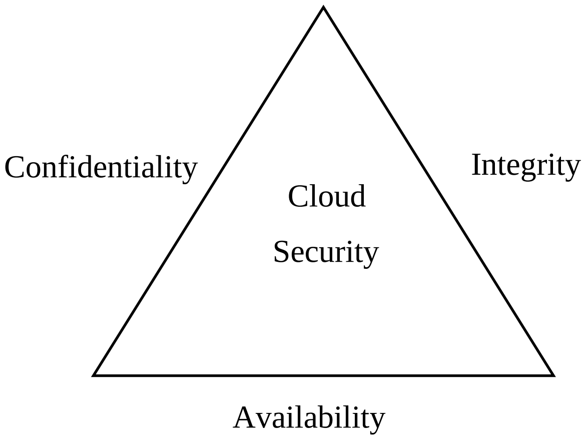


Figure 3: Security in the Cloud as Defined in the CIA Triad
Source: *Author* (2019)

For this research, cloud computing security is defined as ability to safeguard cloud systems and the confidentiality, integrity and availability of the data they contain. This research deals with the perceived uncertainty and risk with the use of the cloud computing and its related applications. The research employs a risk assessment methodology on randomly selected SMEs in Kenya. The empirical data (as illustrated in chapter 4) collected through experiments, questionnaires and strategic interviews are used to build a framework that SMEs could use to benchmark vulnerabilities and to proactively mitigate risks.

2.9.1 Understanding Risk

Risk is the likelihood of the occurrence or realisation of a threat, with a possibility to adversely impact on business. Typically, when risk is calculated quantitatively, the functional values of threats, vulnerabilities and assets are estimated from a probability domain (Miller, 2000; Tan, 2002). Culp (2002) defines risk as any random occurrences with adverse impact or effects on a firm. Risks impacting on organisations could be classified as either exogenous (due to weaknesses external to the system) or endogenous (due to weaknesses within the system).

Risk management entails risk identification, risk analysis and risk mitigation. Bass and Robichaux (2001) posited that risk identification consists of three key components which are criticality, vulnerability and threat. Srinivasan and Abi-raad (2013) reasoned that risk analysis involves both quantitative and qualitative assessments, though a degree of subjectivity is involved in estimating the risk levels. Yazar (2002) posits that the qualitative risk analysis is subject to expert's or the assessor's opinion. Generally, quantitative risk analysis is suitable in situations where historical data is available and it is easy to quantify or estimate incidents.

Srinivasan and Abi-raad (2013) posit that lack of reliable data on security incidents render the use of statistical models ineffective or at least, with great difficulty. SMEs in most of the country lack reliable historical data that could be used for any quantitative risk assessment in terms of cloud security incidents. This was evident during interviews and meetings with the SMEs. Hence, qualitative risk assessment with the use of subjective experts' opinions becomes appropriate.

Also, in cyber-security, new vulnerabilities and threats emerge almost on daily basis and so qualitative assessment may be more appropriate. Here the risks are described as either low, medium, high, or very high. For this research, cloud systems are classified as being insecure, somewhat secure or secure.

The total impact or risk to the SME is not only financial considerations, but also, morale, business output, credibility, investor and customer confidence, corporate image and reputational damage (Sarkar, 2010). The expert decision must take into account both financial loss due to threat realisation and the morale loss on business functionality, as well as the type of business engaged in.

Stajano and Anderson (2002) hypothesise that cloud computing security is essentially risk management. They advocate that it entails identifying:

i. Assets (which are any items of economic value that are to be protected);
ii. Threats (as any agent, condition, or circumstance that can potentially cause harm, loss, damage, or compromise the asset);
iii. Vulnerabilities (as weaknesses that might facilitate the occurrence of a threat);
iv. Attacks (as ways a threat can be made to happen); and
v. Risks (as the expected loss caused by each attack, corresponding to the value of the asset involved and the likelihood that the attack will occur).

It must be noted that each information has a price tag, and thus, requires a certain degree of protection, which is evaluated through security classification. Information is classified based on a number of factors, including stakeholder's experiences, value of information to the SME, governing laws and regulation, etc.

Luhman (2017) posited that determining risk generally amounts to addressing the following questions:

i. What could go wrong?
ii. How many times does it go wrong?
iii. What is the impact on the organisation? Or what are the consequences?

The answer to the first question is a set of threats, presented by exploited vulnerabilities. The second question requires the evaluation of the possibility of occurrences of these threats. The third question estimates the extent and severity of consequences or the impact level of the risk as a result of the exploited vulnerabilities. The issue of how confident or certain the answers to these questions are correct, is dependent upon the inherent uncertainties surrounding the protection of the assets.

2.9.2 Impact

The impact on a system is measured by the extent and severity of the loss caused to the asset upon threat realisation. The extent and severity of the loss is directly proportional to the operational or business value of the asset compromised or attacked (Sarkar, 2010).

The impact on SMEs associated with the exploitation of vulnerabilities such as compromises of customer data, or alteration of data in transit, or denial of service to an authorised entity, can be determined quantitatively.

In view of the associated impact of cloud computing attacks, most businesses, especially large corporations, invest in both physical and technical security controls (Anderson et al., 2013). The impacts have direct and indirect cost implications like cost of mitigation techniques, cost of restoration, reputational damage amongst others. In order to justify the need for spending to improve security, one must first carry out risk analysis on moving to the cloud or running your business with data in the cloud. Two basic types of risk analysis to consider are quantitative risk analysis and qualitative risk analysis. Quantitative risk analysis attempts to assign independently objective monetary values to the components of the risk assessment and to the assessment of potential losses. Conversely, a qualitative risk analysis is scenario-based (Ketel, 2008).

Both Sarbanes-Oxley Act and Basel II Accord emphasise the need for an integral security risk and business risk management as a regulatory requirement.

The impact of a security attack can be financially significant. SMEs lack the resources available to large enterprises, and they often find it harder to recover from an attack. Carnegie Mellon University 2004 report estimates that 99% of all reported intrusions result through exploitation of known vulnerabilities, for which countermeasures is available. Cashell et al. (2004) proclaimed that SMEs in particular lack the security expertise necessary to fend off cloud security attacks. There are very few studies about security audits and solutions on SMEs in developing countries including Kenya. Most security audit researches have either been on specialised protocol and systems or on enterprises in the developed countries (Peng, & Wang, 2008).

2.9.3 Vulnerabilities

By definition, cyber-security vulnerabilities are weaknesses in the systems, networks, infrastructures and applications. ISO 27005 defines vulnerability as a weakness inherent within an asset or group of assets; which usually are exploited by threats agents. An asset is any resource which is value to the organisation for purposes of business operations and continuity.

Vulnerabilities could be categorised into technical, human, physical, operational and business and compliance. Technical vulnerabilities are such flaws as found in the design, implementation and/or configuration of software and/or hardware components of the systems.

Human related vulnerabilities are those associated with end-user vulnerability, gaps in awareness and training, gaps in discipline, unauthorised elevation of privileges, improper termination of access and so on.

Physical and environmental vulnerabilities are insufficient physical access controls, poor citing of equipment, inadequate temperature and humidity controls, inadequately conditioned electrical power.

Operational vulnerabilities are the lack of change management, inadequate separation of duties, lack of control over software installation, lack of control over media handling and storage, lack of control over system communications, inadequate access control or weaknesses in access control procedures, inadequate recording and/or review of system activity records, inadequate control over encryption keys, inadequate reporting, handling and/or resolution of security incidents.

Business continuity and compliance vulnerabilities are the misplaced, missing or inadequate processes for appropriate management of business risks; inadequate business continuity/contingency planning; inadequate monitoring and evaluation for compliance with governing policies and regulations.

The attack can be active when it attempts to alter system resources or affect their operation, so it compromises Integrity or Availability. A “passive” attack attempts to learn or make use of information from the system but does not affect system resources, so it compromises confidentiality.

2.9.4 Threats

Threats are any events or situations or actions that may cause harm or pose risk to an asset (Rees, Bandyopadhyay, & Spafford, 2003). Whenever a security vulnerability or weakness in a system is exploited, a threat is said to be realised, and thus the system is said to be under cyber-attack. The entity that facilitated or caused the attack is known as a threat agent or an attacker. Some threat agents are human, such as end-users (legitimate or illegitimate, intentional or unintentional), often times called hacker or cracker. The other is nature, such as natural disasters.

Some threats may be due to threat agents such as:

i. Deliberate actions by people, be they internal or external to the system.
ii. Accidental actions by people, be they internal or external to the system
iii. System problems - hardware failures, software failures, failures of related systems, introduction of malicious code.

iv. Other problems like power outages, natural disasters.

Threats include unauthorised access to or use of information or assets, cyber-threats that deny, disrupt, degrade or destroy information and assets. They also include the theft of information and computer, viruses, websites defacement, denial-of-service (DoS) attacks, system penetrations, and alteration of data.

Any effective cloud or data security program or initiative includes performance of vulnerability and threat analyses. Herrmann's (2001) vulnerability and threat analyses framework entails the following:

i. To select appropriate cyber-security analysis techniques;
ii. To identify vulnerabilities, their type, source and severity;
iii. To identify threats, their type, source and likelihood; and
iv. To evaluate transaction paths critical to threats zones and risk exposure.

2.10 Related Studies about Cloud Security

Several researchers have conducted work related to the security in cloud computing and some of these researches that are relevant to this research are summarised below.

Popović and Hocenski (2010) in their study presented some standards that can be used to address security issues in cloud computing such as: Information Technology Infrastructure Library (ITIL), International Organisation for Standardisation (ISO 27001/27002) and Open Virtualisation Format (OVF). They also argued that it is very important to take security and privacy into account when designing and using cloud services. The authors concluded that more methods have to be proposed in the future in order to provide a more secure cloud.

Ramgovind, Eloff and Smith (2010) presented guidelines for managing cloud security which include: cloud governance, cloud transparency and cloud computing security impacts. Both studies highlighted the need for standards guidelines for improving security in the cloud.

Chuang, Huang, and Kuo (2011) proposed an Effective Privacy Protection Scheme (EPPS) to provide the appropriate privacy protection for cloud services. EPPS satisfies users' privacy requirements and maintains system performance simultaneously. First, they analysed the privacy level users require and quantified the security degree and performance of encryption algorithms. Then, an appropriate security composition is derived by the results of analysis and quantified data. Their simulation results showed that the EPPS not only fulfils users' privacy requirements but also maintains the cloud system performance in different cloud environments. The execution results show that EPPS outperforms other security schemes by 35% to 50%.

According to Wang, Wang, Ren and Lou (2011), in order to satisfy the assurances of cloud data integrity and availability and enforce the quality of cloud storage services for users, the authors proposed a highly efficient and flexible distributed storage verification scheme with two salient features. By utilising a homomorphic token with distributed erasure coded data, their scheme achieves the integration of storage correctness insurance and data error localisation, i.e., the identification of misbehaving server(s). Unlike most prior work, the new scheme further supports secure and efficient dynamic operations on outsourced data, including: block modification, deletion and appending. Extensive security and performance analysis showed that the proposed scheme is highly efficient and resilient against failure, malicious data modification attacks, and even server collusion attacks.

The work by Wang et al. (2011) studied the problem of ensuring the integrity of data storage in Cloud Computing. In particular, the authors considered the task of allowing a third-party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminated the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for cloud computing.

They stated that a significant step toward practicality is the support for data dynamics via the most general forms of data operation, such as block modification, insertion, and deletion, since services in cloud computing are not limited to archive or backup data only. While prior work on ensuring remote data integrity often lacks support for either public auditability or dynamic data operations, this work achieves both. The authors showed how to construct an elegant verification scheme for the seamless integration of these two salient features in their protocol design (Wang et al., 2011).

In a study conducted by Băsescu et al. (2011), the authors proposed a generic security management framework allowing providers of cloud data management systems to define and enforce complex security policies. They designed the framework to detect and stop a large number of network driven attacks defined through an expressive policy description language and to be easily interfaced with various data management systems. The benefits of preventing a DoS attack targeted towards BlobSeer were evaluated through experiments performed on the Grid5000 testbed.

The work by Kumar and Saxena (2011) investigated the problem of assuring the customer of the integrity of his data in the cloud. The cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised since the data is physically not accessible to the user. The authors provided a scheme which gives a proof of data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. This proof can be agreed upon by both the cloud provider and the customer and can be incorporated in the service level agreement.

A study on security and privacy issues in cloud computing conducted by Wang et al. (2012) suggested four methods for cloud security and privacy including:

i. Access control method which is an application of Role-Based Access Control (RBAC) on cloud computing to produce one algorithm called cloud-based RBAC. The author defined the basic component in this method as: Cloud User, Access Permission, Role and Session. He stated that at the beginning of each session, Cloud Users can request to acquire some of the roles (permissions). If the Role is enabled, some sensitive requests are granted. In this way, the malicious attacks on user data can be prevented as for such activity a user cannot acquire the access permission,

ii. Policy integration method which is a dynamic policy control mechanism that handles the multi-policy problem and dynamically determines the dominant policy during certain data processing,

iii. Identity management method which is used to prevent the unauthorised secondary usage of data. In this method the author added the Cloud Privacy Label (CPL) to the user centric identity management to get a mechanism to protect the cloud users' privacy,

iv. User control method which is a method to solve the problem that the cloud users will lose control of their data as a result of virtualisation. To address this problem the author introduced the Third-Party Auditor (TPA) to balance the power between cloud service providers and cloud users.

The author concluded that his methods can only deal with one or two aspects of cloud security problems so some more methods have to be proposed in the future in order to provide a more secure cloud.

In a study conducted by Delettre et al. (2011), the authors discussed the main cloud computing security risks and focused on the data confidentiality problem in the context of e-commerce clouds. They identified the properties that must be fulfilled to conceal the data of legitimate users and proposed a data concealment component to protect legitimate data and its implementation. This security component is composed of three sub-components, they are:

i. The prediction sub-component which uses a basic but fast and efficient predictive model to define the number of artificial data vectors to insert in addition to the vector marked to conceal the real data,
ii. The data generation sub-component which generates the number of artificial data vectors given by the predictive model,
iii. The data marking sub-component which marks the data vector to insert. The authors evaluated the performance of their security component and found that it successfully conceals data of legitimate users to protect it against potential attackers.

The authors concluded that although their security component is efficient, it is necessary to improve the data marking methods.

Mathisen (2011) also discussed some vital issues to ensure a secure cloud environment. This included a basic view of security policies (inside threats, access control and system portability), software security (virtualisation technology, host operating system, guest operating system and data encryption) and hardware security (backup, server location and firewall). The author concluded that an important issue for the future of cloud security is the use of open standards to avoid problems such as vendor lock-in and incompatibility. Furthermore, the author believes that although there are no security standards specific to cloud computing, conventional security concepts can be usefully applied.

In a research conducted by Sengupta, Kaulgud and Sharma (2011), the authors discussed the security issues in a cloud computing environment. They focused on technical security issues arising from the usage of cloud services. They discussed security threats presented in the cloud such as VM-Level attacks, isolation failure, management interface compromise and compliance risks and their mitigation. They also presented cloud security architecture, using which; organisations can protect themselves against threats and attacks. According to the authors the key points for this architecture are: single-sign on, increased availability, defence in depth approach, single management console and Virtual Machine (VM) protection.

Tripathi and Mishra (2011) tried to categorise the key concerns about cloud security and discussed the technical implications and research issues related to it. They identified four categories of common security issues around cloud computing, they are: cloud infrastructure, data, access and compliance. Additionally, the authors presented a few high-level steps towards a security assessment framework. They stated several observations related to the current status of cloud computing security including: the security standardisation activities are fragmented among many industry forums, quick provisioning of users in the cloud has become complicated, more mainstream research is required in the area of data anonymisation and privacy preserving techniques, adherence to compliance by cloud providers is essential for commercial success of cloud, and migrating generic in-house software to public clouds requires thorough understanding of potential security risks.

Mukhin and Volokyta (2011) analysed vulnerabilities and security risks specific to cloud computing systems. They defined four indicators for cloud-specific vulnerability including:

i. It is intrinsic to or prevalent in core technology of cloud computing,

ii. It has its root in one of NIST's essential cloud characteristics,

iii. It is caused by cloud innovations making security controls hard to implement,

iv. It is prevalent in established state of the art cloud offerings.

The authors were certain that additional cloud-specific vulnerabilities will be identified; others will become less of an issue as the field of cloud computing matures. However, they believe that using a precise definition of what constitutes vulnerability and the four indicators they identified will provide a level of precision and clarity that the current discourse about cloud computing security often lacks.

Most of the work mentioned above seem to focus on certain aspects of the security and privacy problem in cloud computing. In this research, a Framework for Improving Security in Cloud Computing by using security metrics for SMEs is proposed that serves as a comprehensive guidance for achieving higher security level in the clouds and is aligned to the challenges faced by SMEs.

Sometimes SMEs do not consider that they have information assets to protect in the cloud; sometimes they do not know the many tools that modern hackers may use (Saripalli & Walters, 2010). The main issue for SMEs, once they approach the security dimension, is represented by costs: They are not independently able to identify best practices, which allow higher protection levels with minimum effort (Sultan, 2011). As a consequence, these companies risk making a wrong estimate of costs needed for their asset security, and this often make them give up the idea of improving security, with enormous consequent risks, which they are not aware of.

2.11 Review of Frameworks

As new threats emerge, regulations and standards continue to increase in number and complexity. Now, many laws carry penalties for data breaches and for not meeting timely notification of those affected. These areas of concern are addressed as the cloud environment continues to evolve with the utilisation of encryption methods are incorporated as organisations define their strategy for cloud control. The benefits of security frameworks are to protect vital processes and the systems that provide those operations. A security framework is a coordinated system of tools and behaviours in order to monitor data and transactions that are extended to where data utilisation occurs, thereby providing end-to-end security (Vahradsky, 2012).

2.11.1 Cyber Security Framework

The National Institute of Standards and Framework’s Cyber Security Framework (CSF) was published in February 2014 in which the president called for a standardised security framework for critical infrastructure in the United States. The NIST CSF is recognised by many as a resource to help improve the security operations and governance for public and private organisations. While the NIST CSF is a vital guideline for transforming the organisational security posture and risk management from a reactive to proactive approach, it is a difficult framework to understand and implement due to its complexity. The CSF has two primary advantages:

i. **Risk-based approach**. Since the beginning of cyber security, the focus has been on defence. CSF shifts the primary focus to risks as the outcome as opposed to just controls.

ii. **Relevance to Current Threats**. The CSF framework includes important updates that make more relevant today, including authentication and identity, self-assessing cyber security risk, managing cyber security within the supply chain and vulnerability disclosure.

Similarly, the CSF has some shortcomings as mentioned below:

i. **Complexity**. There is not much information provided on how companies can automate some of the implementation steps for this framework (Pleshakova, 2018) As the cyber security world continues to evolve and change, automation is key for resource allocation and, as a result, a better security posture.

ii. **Developed for Critical Infrastructures**. The CSF was developed for critical infrastructure community and is not readily fitting into the SME environment or cloud security environment. CSF would be yet another security checklist that smaller organisations would ignore due to its complexity (Hayden, 2010). By following this framework, organisations are assumed to have less risk but this framework still does not help to measure cloud risks in tangible terms. According to Shackelford, Russell and Haut, (2015) the functions, categories or sub categories in the latest NIST CSF draft do not specifically call out or even attempt to address cloud related risks.

2.11.2 ENISA Cloud Framework

The Cloud Security Alliance and European Union Agency for Network and Information Security (ENISA) have compiled a set of recommendations in a cloud security framework for European Union (EU) governments. The recommendations discuss some EU- and government-specific topics, such as the possibility of a European Government Cloud and an assessment of EU member cloud maturity, but most of the report is generally applicable to cloud security across application domains.

The framework outlines a four-stage lifecycle for developing and deploying clouds, which includes planning, implementing, review and evaluation, and remediation. The ENISA framework has two primary advantages:

i. **Monitoring and Logging**: The framework stresses on this as a critical aspect since monitoring and auditing may detect weaknesses in current practices and implementations.

ii. **Exit management:** Exit management is especially important to manage transitions when a government or enterprise terminates a cloud contract. A number of critical areas should be addressed when planning for exits, including how data will be deleted, how access control and identity information will be protected, and how services continuity will be maintained. The framework encompasses this aspect soundly.

The ENISA framework has some shortcomings as mentioned below:

i. **Relevance:** The framework is less relevant to enterprise cloud users due to its complexity and also the fact that it is more significant to government clouds. The framework does not account for challenges encountered by developing country SMEs. For example, the challenges of availability due to internet outages. The framework is aligned for the EU countries.

2.11.3 International Standards Organisation (ISO) 27001

The ISO 27001 is one of the most widely known security standards and is a mature framework focused on information security. It’s very comprehensive and broad, and can be used across a wide range of types and sizes of businesses.

Because it’s tried and tested, countries often use it as a basis on which to create a manual about security and what to do. However, like many of the ISO standards, it can be a bit daunting, and many smaller organisations are put off by the effort required to gain accreditation and the perception that it can be difficult to implement.

According to a research conducted by Muthee (2013), only 5% of organisations in Kenya have certified with ISO 27001 and the number is less than 1% for SME. This is due to the fact that organisations see it as both technically and procedurally challenging, adding additional overhead to their business.

Based on the studies on cloud security and existing frameworks reviewed above, it is noted that a suitable framework for SMEs to self-assess their cloud security is not available either due to their complex nature in adopting them or because they do not cover the cloud aspect effectively.

2.11.4 COSO Framework

The Committee of Sponsoring Organisations of the Treadway Commission (COSO) came up with a model that evaluates internal controls. This model has been adopted as the generally accepted framework for internal control and is widely recognised as the definitive standard against which organisations measure the effectiveness of their systems of internal control. The COSO model defines internal control as a process that is achieved by an entity’s executive management, operations management and other users. The framework was designed to provide assurance of the attainment of points in the following categories:

ii. Effectiveness and efficiency of operations
iii. Reliability of financial reporting
iv. Compliance with applicable laws and regulations

In an effective internal control system, the five components work to support the achievement of an entity’s mission, strategies and related business objectives. The five functions are control environment, risk assessment, control activities, information and communication and finally monitoring.

The COSO framework individually does not solve the issues arising from security in the cloud. This is because the framework is focused on just one area of the organisation of the internal controls and therefore might not be cloud ready.

As indicated in the above section, framework and guidelines like ISO 27001, NIST 800-53, ENISA and COSO have been reviewed, but all these standards are in evolving stages for the Cloud computing environment. Although ISO/IEC 27001 provides generic guidance in developing the security objectives and metrics, but it still does not provide methods to guide SMEs and is very general.

Apart from this, the security requirements of SMEs vary based on their specific security risks. Therefore, it is vital to have a standardised security framework based on industry standards, but tailored to the specific requirement of SMEs. While reviewing industry security framework and guidelines, it was found out that there are no cloud security frameworks, best practices and guidelines aligned towards the challenges faced by SMEs either due to their complex nature in adopting them or because they do not cover the cloud aspect effectively.

2.12 Basics of the Framework for Cloud Security

Typically, the security objective is to deter, prevent, detect, recover from, and respond to threats arising from the usage of cloud computing. Cloud security is to safeguard these information assets, the information systems and networks that deliver the information to and from the cloud, from damage or compromise resulting from failures of confidentiality, integrity and availability. Security is multifaceted and it includes information technology, procedures and practices, laws and regulations, people and organisations; these areas are said to be interrelated and impact each other (Denning, 2003).

To ensure business continuity, SMEs require a means that enables them to proactively analyse the various imperative factors critical to the security and business operations.

The proposed Framework for Improving Security in Cloud Computing for SMEs (FISCCS), as defined in this research borrows its core from the Cyber-security Framework (CSF). This choice is based on the fact that the Framework, deriving from the NIST, provides a full coverage and is at the state of the art of the life-cycle of information and system security, however, because it has been created from Critical Infrastructures made up of 21 Categories and 98 Subcategories, it introduces a complexity level which is not suitable for most SMEs of the developing nation and therefore Kenyan context.

The proposed Framework for Improving Security in Cloud Computing for SMEs (FISCCS) borrows some concepts from the Cyber-security Framework (CSF) represented in Figure 4.

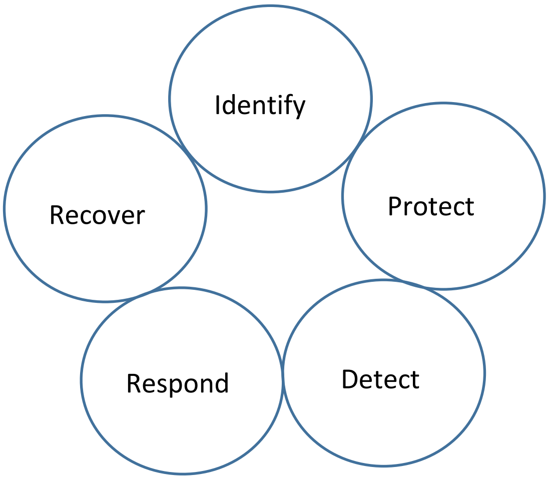


Figure 4: Cyber-Security Framework
Source: *The National Institute of Standards and Technology (2014)*

The 5 Functions are briefly described below:

i. **Identify**: The Identify function is linked to the understanding of the company context, of assets that support the critical business processes and relevant associated risks. Such understanding enables the SME to define resources and investments according to the risk management strategy and company objectives. The Categories within this Function are: Asset Management; Business environment; Governance; Risk analysis; Risk management strategy.

ii. **Protect**: The Protect function is linked to the implementation of measures aimed at protecting the data and its movement to and from the cloud. Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

iii. **Detect**: The Detect function is linked to the definition and implementation of appropriate activities aimed at identifying IT security incidents on time. Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

iv. **Respond**: The Respond function is linked to the definition and implementation of appropriate activities in order to take action in case of detection of a cyber-security event or attack. The aim is to reduce the impact of a potential cyber security event. Categories within this Function include: Planning; Communications; Analysis; Mitigation; and Improvements.

v. **Recover**: The Recover function is linked to the definition and implementation of activities aimed at the management of plans and activities to restore processes and services impaired due to a cyber-security event. The aim is to ensure the resilience of systems and facilities and, in case of incident, to support the timely recovery of business operations. Categories within this function include: Recovery Planning; Improvements; and Communications.

As any company risk, the risk of data in the cloud cannot be eliminated and therefore requires a series of coordinated actions to be taken in order manage it. Such actions involve the organisation and technology departments of the company, in addition to the financial management of the risk, also through the establishment of a residual risk management strategy and a strategy to protect the company balance.

Furthermore, the cyber risk is intrinsically highly dynamic. It changes as threats, technology and regulations change. To start approaching this issue in a way which is useful for the developing country systems (state, enterprises and citizens) it is necessary to define a common ground, a Framework, in which the various production sectors, government agencies and regulated sectors can recognise their business, so to align their cyber security policies in a steadily developing process.

To reach this aim a common Framework should be first of all neutral both in terms of business risk management policies and in terms of technology, so that each player could keep on using its own risk management tools, managing its technology assets while monitoring at the same time the compliance with sector standards.

This study presents a Framework for Improving Security in Cloud Computing for SMEs (FISCCS) aimed at creating a common language to compare the implementation of these systems risks. The framework may well help an SME to plan a cloud risk management strategy, developed over the time according to their business, size and other distinguishing and specific elements of the SMEs.

The choice to develop the framework is based on the idea that the answer to threat management should provide an alignment at international level, not only at national level. The framework offers high flexibility, which is mostly targeted at SME facilities; and was developed according to the characteristics of the social and economic system of our country, reaching a cross-sector framework that can be contextualised in implementation of secure cloud for SMEs. This allows the transfer of practices and knowledge from one sector to another in an easy and efficient way.

In this sense, this study introduces three important concepts in the Cyber-security Framework (CSF) Framework:

i. People involved in handling the data in the cloud, the cloud users, the administrators as well as the owners of the SME who make decisions and invest into IT security. The people element represents the human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. It represents a human collective and must take into account values, behaviours and biases. It is critical for the IT administrators or IT managers to work with the human resources and legal departments to address employment issues including access to tools and data, training and awareness, privileges within the enterprise and its IT assets. Other issues that may need to be addressed include recruitment strategies (access, background checks, interviews, roles and responsibilities) and termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to other employees).

ii. Technologies for securing data in the cloud available to the SMEs, these include two-factor authentication for logging into the cloud, use of encryption for data at rest, transport later security (TLS) for data during transport over the network, secondary link for failover to prevent lockout among others. Given the typical enterprise's dependence on technology, technology constitutes a core part of any SMEs infrastructure and a critical component in accomplishing its mission. Technology is often seen by the enterprise's management team as a way to resolve security threats and risks. While technical controls are critical in mitigating certain types of risks, technology alone should not be viewed as an information security solution.

iii. External factors affecting the usage of cloud including government laws, cloud owner data retention policies, offshore backups by cloud providers.

The integration of these components is represented in the framework as shown in Figure 5:

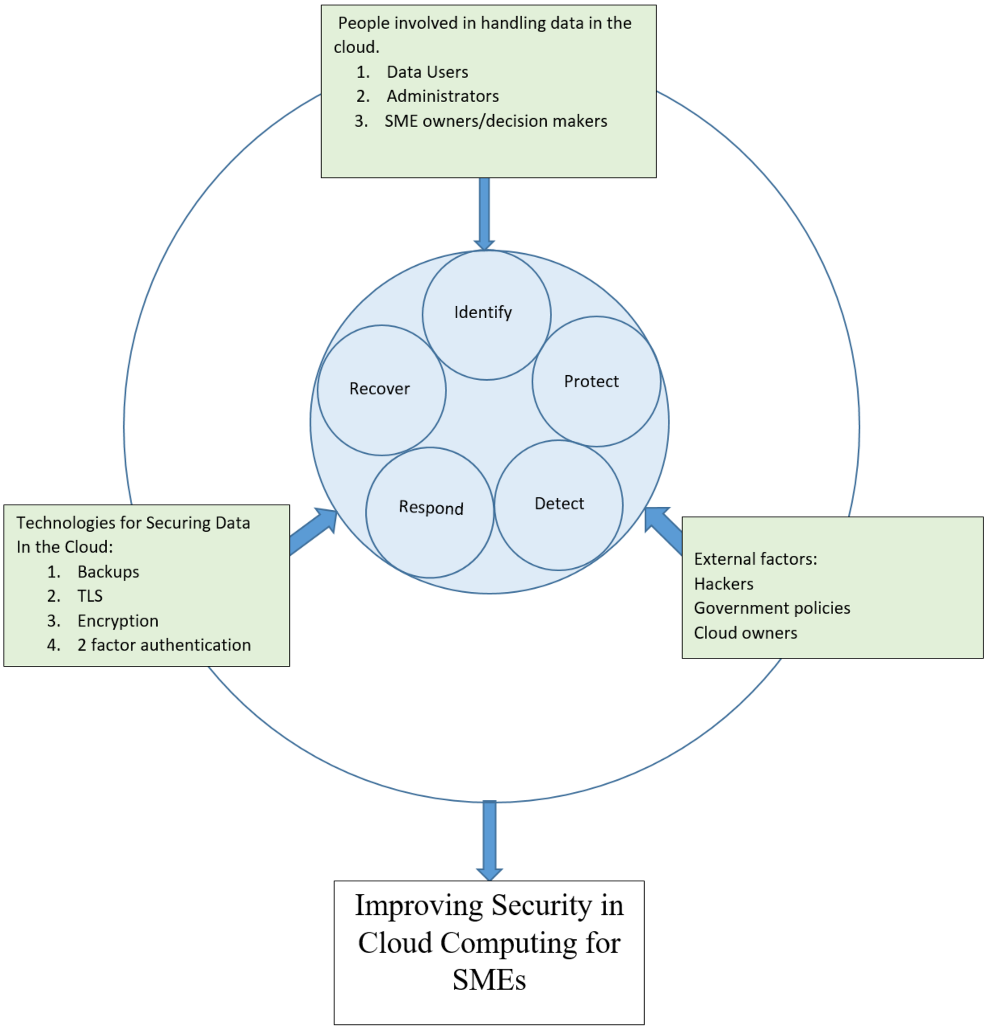

People involved in handling data in the cloud.
1. Data Users
2. Administrators
3. SME owners/decision makers
Identify
Recover
Protect
Respond
Detect
Technologies for Securing Data In the Cloud:
1. Backups
2. TLS
3. Encryption
4. 2 factor authentication
External factors:
Hackers
Government policies
Cloud owners
Improving Security in Cloud Computing for SMEs

Figure 5: Building the Framework
Source: *Author (2019)*

2.13 Conceptual Framework

This research studies demonstrates the possible application of a Framework for Improving Security in Cloud Computing for SMEs (FISCCS) by specifically adding the independent variables of people, technology and external factors to the dependent variables of the cloud security cycle to achieve secure cloud computing for Software as a Service.

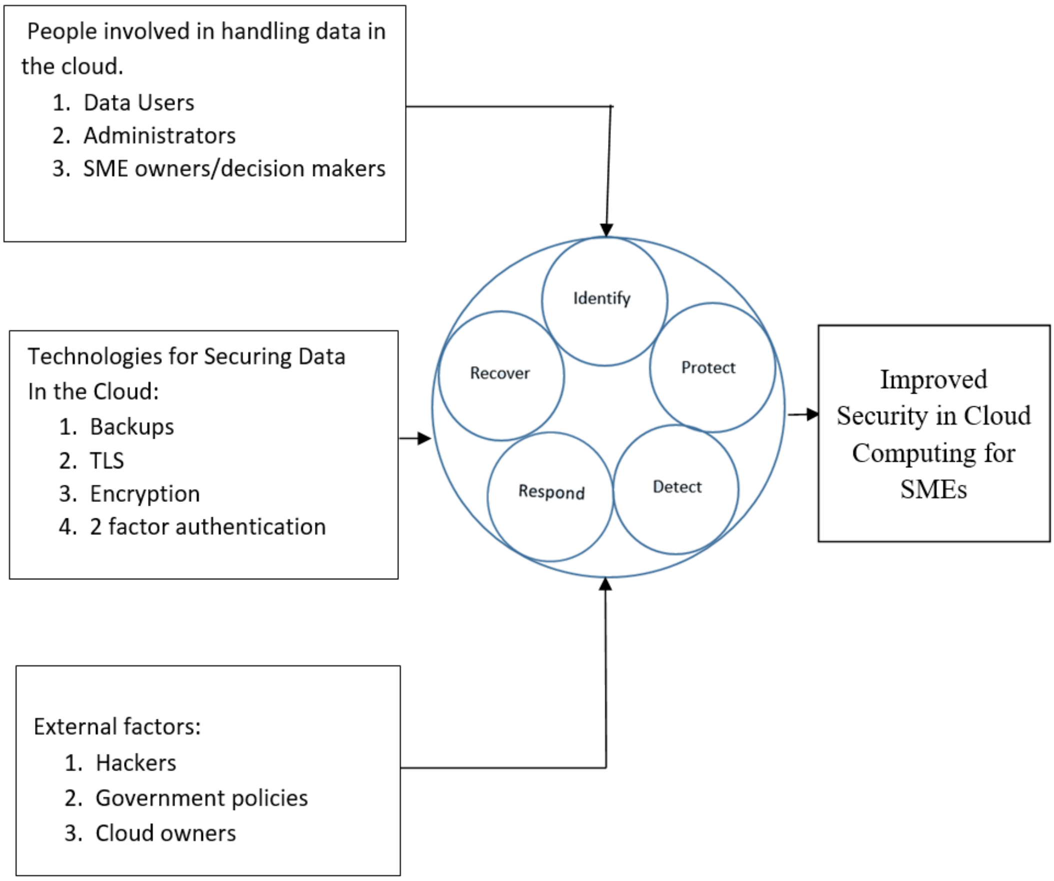
The independent and dependant variables for the research are broken down as indicated in Table 1 below:

Table 1: Conceptual Framework Building Blocks

Independent Variables	Intervening Variables	Overall Dependent Variable
People	**Identify** Risks in Cloud	Security in Cloud Computing for SMEs
Technology	**Protect** Data in the Cloud	
External Factors	**Detect** Security Incidents in the Cloud	
	Respond to Threats in the Cloud	
	Recover from Breaches in the Cloud	

Source: Author (2019)

The conceptual framework is depicted in Figure 6 having achieved the goal of Improving Security in Cloud Computing for SMEs.



People involved in handling data in the cloud.

1. Data Users
2. Administrators
3. SME owners/decision makers

Technologies for Securing Data In the Cloud:

1. Backups
2. TLS
3. Encryption
4. 2 factor authentication

External factors:

1. Hackers
2. Government policies
3. Cloud owners

Figure 6: Conceptual Framework
Source: *Author* (2019)

2.14 Chapter Summary

This chapter started by outlining the properties and advantages of cloud computing as well as describing its importance for the SMEs in detail. The chapter further highlighted the cloud computing security challenges, threats and risks as related to SMEs. Further to this, other frameworks were discussed highlighting their strengths and shortcomings and similar studies in the same field are also reviewed. To sum up the chapter, the conceptual framework was formulated showing the perception of the problem and how variables operate in influencing each other. This also graphically presented the independent and dependent variables of the research as well as the intervening variables.

CHAPTER THREE
RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

This chapter describes the research methodology adopted for the study. It covers research design and reasons for its choice in the investigation of the research problem area given. Further, it describes the target population, sample size, sampling procedures, instruments, data collection procedures, validity, reliability and data analysis. This chapter also describes the practical method used in developing a Framework for Improving Security in Cloud Computing for SMEs. The research design adopted in this study aims to assist in answering the research questions of this thesis. The research was conducted in three steps as below:

i. Descriptive research to gather views of current cloud security challenges faced by SMEs using questionnaires.
ii. Experimental research to determine the backend cloud vulnerabilities and threats by using OwnCloud as a research tool.
iii. Proposed a theoretical framework for use by SMEs to secure their data in the cloud using the Goal-Question-Metric (GQM) methodology.

3.2 Research Design

Oso and Onen (2011) have described a research design as a plan on how the researcher intends to conduct the research while Donald and Delno, (2006) have also noted that a research design is a framework of how data was collected and analysed in an investigation. Research design therefore provides the most valid and accurate answers to research questions.

This study adopted a mixed research methodology comprising of experimental and descriptive research designs. Descriptive research is a study designed to depict the participants in an accurate way and describes people who took part in this study (Kowalczyk, 2015). This approach assisted the researcher to analyse and define the security of SaaS cloud computing among the top 100 SMEs in Kenya. This involved using a questionnaire to collect views of staff in the SMEs.

Descriptive survey was therefore chosen for this study because the researcher was interested in the opinions of the respondents in terms of security challenges in cloud computing. Descriptive research design enabled the researcher to generalise the findings to a larger population. The research in this case generalised the security challenges of cloud computing among SMEs in Kenya. In addition, the study adopted a mixed method approach in which both qualitative and quantitative data were collected. Combining both quantitative and qualitative data enabled the researcher to best understand and explain a research problem (Creswell, 2014).

This procedure seemed to capture the complexity of SMEs of their workplace conditions. Therefore, a combination of quantitative and qualitative research was a better option. Interviews assisted in achieving a more behaviourally related assessment of the participants' lives at work and a better indication of the exact factors that contributed to their levels job dissatisfaction (George, Louw, & Badenhorst, 2008).

In experimental research design, the researcher gathered vital information regarding the possible technical challenges and vulnerabilities in cloud computing by using a private SaaS cloud called OwnCloud. The private cloud platforms were subjected to operation in the same SME environment whereby users stored data and general security vulnerabilities were identified.

Finally, the GQM methodology was used to formulate the cloud computing security metrics hierarchy. The main goal of the hierarchy was to produce a security index that describes the security level accomplished by the evaluated cloud computing environment. In part because there are no universally recognised metrics for cloud security, it is very important that organisations adopting cloud infrastructures carefully develop measurements appropriate to their unique strategies and goals. A useful method for developing metrics that successfully align with specific strategic objectives is the Goal-Question-Metric (GQM) framework.

It must be noted herewith that this thesis deals with the metrics of cyber-security which is intangible. Measuring cloud security properties is not done in the same manner as a physical property is experimentally measured or observed. Cloud security metrics and indicators are applied to assess security processes and to find the means by which the security posture can be improved and/or managed proactively. Cloud security metrics must be aimed at effective data collection and data analysis with good understanding of its effects on security and business operations.

The purpose of the measurement process is to transform metric data through data analysis into security knowledge to support risk decision-making; which must be inferred or referenced in respect of its sources, such as perceptions of cloud security functionaries or perceived expert's opinions.

3.3 Location of Study

The primary area of study for this research was Nairobi, Kisumu and Mombasa as shown in Table 2. These three cities were selected for the study as they inhibit the major share of SMEs that utilise IT resources for infrastructure growth. The cities are also well connected in terms of internet increasing the rates of SaaS cloud computing adoption as compared to smaller towns. This makes it suitable for conducting research on cloud computing security.

The SMEs were selected using purposive sampling technique so that the researcher can reflect the subject of the matter that needs to be studied. Purposive sampling is a sampling method where the sample is selected based on characteristics of a population and the objective of the study.

3.4 Population of the Study

A population refers to a group of individual persons, objects or items from which samples are taken for measurement (Creswell, 2014). The target population for this study was the top 100 SME companies in Kenya as of 2016. This target population was chosen purposively for this research because these companies have sensitive and crucial data that needs to be kept secure and private as well as utilise IT resources for infrastructure growth. The companies consist of those in the manufacturing, hospitality, health and finance sectors and are currently using cloud computing or considering the use of cloud computing due to their infrastructure size and requirement. The SMEs had people participating in the research that filled in the questionnaire. These included the directors or CEOs, finance in charge, IT administrators and data/system users. Finally, the sample population of SMEs are selected to meet the following criteria:

i. SMEs with number of employees not exceeding 250;

ii. SMEs must be in Kenya;

iii. SMEs must use the cloud computing for business data storage and/or operations;

iv. SMEs must have at least one employee in charge of ICT or technical operations or a chief-level officer responsible for operations.

3.5 Sampling Techniques and Sample Size

Sampling procedure refers to the process and function of selecting a sample that represent a given population. In order to determine the sample size of SMEs to be drawn from the 100 SMEs in the study area, the study adopted a formula from Nassiuma (2000) using the coefficient of variation for estimating a sample size, n, from a known population size, N.

$$n = \frac{NC^2}{C^2 + (N - 1)\, e^2}$$

Where n= sample size

N= population, 100 SMEs in this case.

C= Co-efficient of variation, assumed to be 22%.

e = Standard error, assumed to be 0.02 in this case.

Therefore, $n = \frac{100 \text{ X } 0.22^2}{0.22^2 + (100-1)\ 0.02^2}$

n=16.388 (rounded off to 16)

For the purpose of this study, 16 companies were sampled under different sectors which included manufacturing, hospitality, health and finance sectors. The SMEs were selected using purposive sampling from the areas as shown in Table 2.

Table 2: Sampling Frame

City	No. of SMEs from top 100	Sample Size
Nairobi	80	9
Kisumu	9	5
Mombasa	7	2
Rest of Kenya	4	0
Total	**100**	**16**

Source: *Author (2019)*

Purposive sampling technique was used to sample the 16 SMEs that had the characteristics the researcher was looking for; having sensitive and crucial data that needs to be kept secure and private as well as utilise IT resources for infrastructure growth. The choice of purposive sampling technique is prompted by assertion that purposive sampling is one in which persons are deliberately selected for the vital information they can make available that cannot be obtained from other choices (Padgett, 2016).

The Rest of Kenya depicts smaller towns and these were not included in the sample size but are illustrated on Table 2 for understanding purposes. Members of SMEs who were selected to participate in the study were those that were directly involved with data and decision making of the SMEs. From each of the 16 sampled SMEs 15 people were purposively selected to participate in the study. Therefore, the sample size used in this study was 240 respondents. The distribution is as shown in Table 3.

Table 3: Members of SMEs participating in the Questionnaire

Department	**Number of respondents**	**Total number of respondents (No. of respondents X 16)**
Directors/Owner/CEO	1	16
Finance controller	1	16
Accounts department	3	48
IT admins/technicians/IT staff	5	80
Data user/ System user	5	80
Total	**15**	**240**

Source: *Author* (2019)

3.6 Instrumentation

Typical threats that exist in the cloud from the backend or cloud providers' side are unknown to the SMEs and even unavailable for research due to the cloud providers risking their reputation. Therefore, the researcher simulated a platform of cloud infrastructure using OwnCloud. This platform offers SaaS simulation for private cloud computing and is widely accepted and used as a private SaaS cloud computing both for education and commercial purposes. The requirements for the system are described as below:

3.6.1 Infrastructural Requirements

The system requirements for setting up the cloud software for OwnCloud include one server with at least 2 CPU cores, 512MB RAM and local storage as needed. For this research, a 1TB hard disk was used. For this research, a virtual machine was used to install both the cloud servers for a test environment.

3.6.2 Software Requirements

The cloud software works on Linux as the underlying operating system. The SME respondents who participated in the simulation of the study used Windows computers as well as Android mobile phones to save and access their data.

3.6.3 Design of OwnCloud for Experiment

To simplify the environment, the systems were hosted online to run a file server with various users and end user access was provided through a web platform. The file server was used to provide remote file storage and sharing. Different groups of users representing different SMEs were given full access to their own storage area while they were restricted from accessing the other SME's storage areas on this file cloud server. The researcher then tested the above cloud infrastructures against the typical internal threats.

3.6.4 Validation of the Framework

The framework was validated by cross checking against the international security standards COBIT, ITIL and ISO frameworks.

COBIT is a good-practice framework created by international professional association ISACA for information technology management and IT governance. COBIT provides an implementable set of controls over information technology and organises them around a logical framework of IT-related processes and enablers.

ITIL describes processes, procedures, tasks, and checklists which are neither organisation-specific nor technology-specific, but can be applied by an organisation for establishing integration with the organisation's strategy, delivering value, and maintaining a minimum level of competency. It allows the organisation to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

Further to the above, face validity was used to validate the framework. A model that has face validity appears to be a reasonable imitation of a real-world system to people who are knowledgeable of the real-world system. Face validity is tested by having users and people knowledgeable with the system examine model output for reasonableness and in the process identify deficiencies. An added advantage of having the users involved in validation is that the model's credibility to the users and the user's confidence in the model increases.

3.6.5 Questionnaire Design

The questionnaire was structured and mainly self-completion in nature; that is, the respondents were required to answer the questions themselves unaided (independently). The study adopted and administered a set of mixed closed ended questions. Though the questions were the closed-ended type, in few instances it was necessary to ask for the respondents for their independent opinions.

3.7 Reliability and Validity Analysis

According to Creswell (2014) reliability of an instrument is the measure of the degree to which a research instruments yields consistent results or data after repeated trials. Thus, reliability refers to consistence of measurement of the magnitude to which the results are similar over different times of data collection and the extent to which the measures are free from error.

Oso and Onen (2011) observe that in investigating test reliability of research questionnaire several methods such as; test-retest reliability, split-halves, parallel forms and internal consistency can be used. Internal consistency measures consistency within the instrument and questions how well a set of items measures a particular behaviour or characteristic within the test.

According to Oso and Onen (2011), the most popular method of testing for internal consistency of a Likert-scale-itemed questionnaire is Cronbach’s alpha coefficient. It’s the most standardised test of inter-item consistency reliability. It defines the degree to which an instrument is error free, reliable and consistent across the various items in the scale. Hence, the Cronbach’s alpha coefficient test was used to measure the internal consistency of the questionnaire in this study.

Table 4: Internal Consistency: Cronbach's Alpha Results for the Questionnaire

Scale	No. Items	Cronbach's alpha	Cronbach's alpha based on standardised items
Security Challenges	8	.783	.811
Security Measures	8	.623	.578
Concerns on Cloud Computing	7	.712	.698

Source: *SPSS Analysis*.

Table 4 revealed that all the sub-scales met the required level of internal consistency of reliability, with the Cronbach's alpha values ranging from a low of 0.623 (security measures items) to a high of 0.783 (security challenge). These findings were in line with the rule of thumb proposed by Frankel and Wallen (2009) that; a coefficient of 0.60 is an average reliability while coefficient of 0.70 and above indicates that the instrument has a high inter-item consistency reliability standard.

The Cronbach's alpha for all the sub scales revealed that the questionnaire had adequate reliability for the study. Deleting any of the items in the sub-scales would not result to further increase in Cronbach's alpha, that is, it would not cause improvement in the internal consistency. It was also noted that all items correlated with the total scale to a good degree. Hence, the questionnaires were generally suitable for data collection because they adequately measured the constructs for which they were intended to measure.

Internal validity of the constructs was tested by subjecting the survey data to suitability tests using the Kaiser-Meyer-Oklin measure of sampling adequacy (KMO Index) and the Bartlett's Test of Sphericity. This internal validity of the constructs was tested for each sub-scale, as summarised in Table 5.

Table 5: KMO and Bartlett's Test of Internal Validity

Subscale	Kaiser-Meyer-Olkin (KMO index)	Bartlett's Test of Sphericity		
		Approx. Chi-Square	df	Sig.
Security Challenges	.714	330.715	15	.000
Security Measures	.734	278.234	15	001
Concerns on Cloud Computing	.842	351.351	15	.000

Source: *Survey data (2018), SPSS Analysis*

From Table 5, the value of Bartlett’s test of Sphericity is significant ($p \leq 0.001$) for all the sub-scales of the questionnaire. In addition, the Kaiser-Meyer- Olkin indexes are all > .6 which is a threshold for a sufficient internal validity. Creswell (2014) asserts that if the Bartlett’s test of Sphericity is significant and if the Kaiser-Meyer-Olkin measure is greater than 0.6, then condition of adequate internal validity is met. Given the results of the validity tests met these conditions, it implies that questionnaire was of required validity levels and data collected were suitable for inferential analysis.

3.8 Data Collection Procedure

The researcher first of all obtained a letter of introduction from the Dean, School of Computer Science and Bioinformatics of Kabarak University which enabled him to apply for a research permit from the National Commission for Science, Technology and Innovation (NACOSTI) to conduct the study. The researcher then went to the sampled SMEs offices to seek for permission from the Directors/Owner/CEO of institutions to conduct the study in their organisations and for introduction and familiarisation with the organisations’ administration and would be respondents.

The researcher then met the respondents to clarify to them the basis for the study and assured them of confidentiality of their responses and freedom to withdraw from the study if any of them felt uncomfortable. Participants were taken through necessary instructions and were given approximately 10-15 minutes to fill the questionnaires.

3.9 Data analysis

Data was analysed in two perspectives. First, the data obtained using questionnaires was analysed using descriptive statistics. The findings were presented using graphs, tables, charts, frequencies and percentages. The second phase of the analysis consisted of presenting experimental results after simulation of OwnCloud.

Goal Question Metrics method was used to construct the framework which provided the cloud security status for SMEs as an output.

3.10 Framework Building through Metrics

Security metrics are measurements from which to monitor and compare the level of security and privacy attained, as well as the current security status of a computing environment. The use of security metrics promotes transparency, decision making, predictability and proactive planning (Hayden, 2010). Metric is a measurement standard, defining both what is being measured (the attribute) and how it is measured (the unit of measure) (Herrmann, 2007).

Measurement is the process of metric collection which, through pre-established rules, will allow the interpretation of results (Herrmann, 2007). Metrics can be composed of sub-elements that are referred to as primitive metrics or sub-metrics. Any restrictions or controls relating to the primitives are defined in the measurement process. A metric can be expressed in one of the following ways:

i. # - `Number` - expressing an absolute value of any element measured;

ii. % - Percentage - expressing a percentage of an element measured in relation to the total number of elements;

iii. Logic value - expressing Yes or No for an event.

Figure 7 represents the proposed life cycle of security management for cloud computing environments.

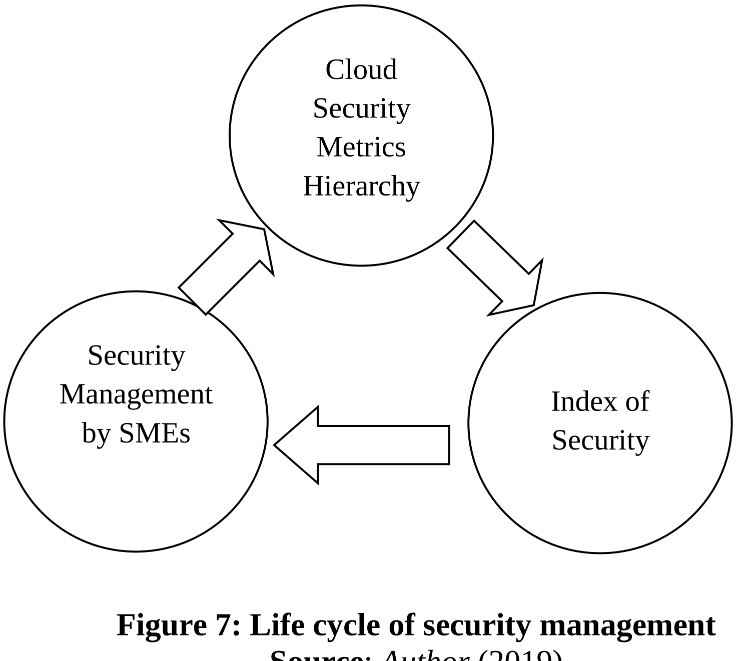


Figure 7: Life cycle of security management
Source: *Author* (2019)

The proposed methodology for security management in cloud computing is based on the following components:

1. Cloud security metrics hierarchy;
2. Index of Security (IndSec);
3. Security Management by SMEs.

A security metrics hierarchy is derived from the GQM methodology. A security index (IndSec) will be computed using the security metrics hierarchy. Finally, the SME will use the security index as a reference for the improving their security. In the context of the life cycle of security management (Figure 7), a security metrics hierarchy is presented as a new form of visualisation of security-related information that is collected from the cloud computing environment.

In the 1970s, the GQM method (Goal Question Metric) (Caldiera, & Rombach, 1994) was designed to move testing for software defects from the qualitative and subjective state it was currently in to an empirical model, in which defects would be measured against defined goals and objectives that could then be linked to results.

The GQM methodology defines a measurement model on three levels:

i. Conceptual level (goal) - a goal is defined for an object for a variety of reasons, with respect to various models of quality, from several points of view and relative to a particular environment.
ii. Operational level (question) - a set of questions is used to define models of the object under study and then attention is focused on that object to characterise the assessment or achievement of a specific goal.
iii. Quantitative level (metric) - a set of metrics, based on the models, is associated with every question in order to answer it in a measurable way.

In this research methodology, the security metrics hierarchy is generated directly from the GQM definition process, during which stage security features are mapped to corresponding security metrics. Table 6 shows the relationship between the GQM methodology and the security metrics hierarchy (SMH).

Table 6: Relationship between the GQM methodology and SMH

GQM Levels	**SMH Levels**
Conceptual level	Group Metric
Operational level	Metric
Quantitative level	Sub-Metric

Source: *Security Metrics Hierarchy (2019)*

For each goal statement identified in the conceptual level, a group metric was defined. The operational level identifies which objects or activities must be observed or collected to measure the individual components of the goal statement. Lastly, the quantitative level defines which metrics remains explicitly aligned with the higher-level goal statement.

The security metrics hierarchy is derived from the GQM methodology. The metrics are classified into Group metrics, Metrics and Sub-Metrics as shown in Figure 8.

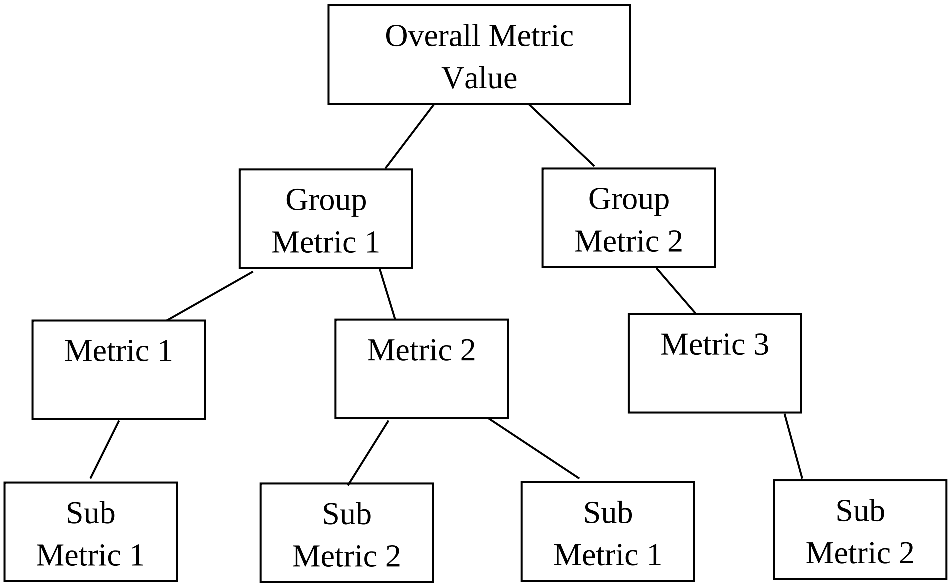


Figure 8: Metrics Classification
Source: *GQM Methodology (2019)*

The sub-metric represents a sub-part of a metric; it is used when a metric can be specialised in several ways, with each one having a different contribution to the overall metric. The importance of value conversion is to extract a meaning for the values measured by the primitive metrics. Further, value conversion helps to prevent the value domains of security metrics from having instances that are difficult to be compared with each other, and to simplify the computational model using a method to converge the values of each primitive metric measured to a common scale of values.

A metric of type logic must return a logical value measured from an event, for instance, does the cloud have a 2-factor authentication for authorising users? The conversion function is described as $y = f(x)$, where x can be a measured logic value Yes or No:

$$y = \begin{cases} 1 \text{ if } x = \text{Yes} \\ 0 \text{ if } x = \text{No} \end{cases}$$

Beginning with goals, the researcher defined the strategic objectives for cloud security based on the feedback from the SMEs. These goals naturally trigger questions that must be answered to determine whether the goal has been met. For instance, if the goal is ensuring that a cloud provider is protecting sensitive data as well as the consumer, certain questions emerge: How well does the consumer protect data today? How well does the provider protect internal data? What controls are in place in the SME? Many questions emerge, all representing the process by which the SME verifies performance against the goal. Questions in turn trigger demands for data and measurement.

3.11 Ethical Considerations

An introductory letter was obtained from the Board of Postgraduate Studies, Kabarak University. In addition, Research authorisation was sought from National Commission for Science, Technology and Innovation (NACOSTI). Respondents were well informed on the purpose of the study and those participants interviewed signed the consent form. Participation was voluntary as should be the case for researches (Creswell, 2014). Confidentiality and anonymity were assured and respondents were identified with coded names. All respondents involved in the research both for the purposes of data collection and simulation were assured of confidentiality of the information they gave. Respondents of questionnaires and interviews did not write their names while those that were interviewed were protected as they were masked, pseudonyms were used and were only used for the study and nothing else and were destroyed upon completion of the study. The researcher appropriately informed them that information gathered during the study would be used solely for academic purposes only.

3.12 Chapter Summary

This chapter described the research methodology adopted for the study. It covered research design and reasons for its choice in the investigation of the research problem area given. Further, it describes the target population, sample size, sampling procedures, instruments, data collection procedures, validity and data analysis. This chapter also described the practical method used in developing the Framework for Improving Security in Cloud Computing for SMEs using GQM methodology. Beginning with goals, the researcher defined the strategic objectives for cloud security based on the feedback from the SMEs. These goals were used to trigger questions which form part of the framework.

CHAPTER FOUR

DATA ANALYSIS, INTERPRETATION AND DISCUSSION

4.1 Introduction

This chapter presents the findings and interpretation of the study. The data was collected using questionnaires as well as experimental analysis using open source software OwnCloud. Hence, the chapter has been sub-divided into two sections; first, the experimental analysis of the cloud security which highlights potential threats from the cloud providers' end and second, the quantitative data which highlights the threats from the SME perspective.

The researcher presented the research findings on the basis of the study objectives and research questions. The quantitative data was analysed using descriptive statistics. The descriptive statistics was used to describe and summarise the data in form of graphs, tables, charts, frequencies and percentages. For the qualitative data a thematic analysis approach was used. The Statistical Package for Social Sciences (SPSS) version 20 was used to analyse the data.

On experimental analysis, using open source software OwnCloud a new domain name "www.rupra.co.ke" was setup for this purpose and OwnCloud was setup on it. Accounts for users were setup on the SaaS cloud platform and given to different users to save dummy data into their accounts. Experimental analysis was then carried out with the stored data to identify potential security risks in the cloud.

4.2 Demographic Information of the Respondents

This section represents the demographic information on the respondents including their age, gender, education level and experience.

4.2.1 Questionnaire Return Rate

Table 7, which shows the summary of return rate of questionnaires from the respondents, reveals that the questionnaires were adequate for the study.

Table 7: Questionnaire Return Rate

Respondents	Questionnaires administered	Questionnaires returned	Return rate (%)
Staff of SME	240	202	84.2

Source: *Survey data (2017)*

Out of the 100 SMEs in Nairobi, Mombasa and Kisumu a sample size of 240 staff were selected for the study and were all given study questionnaires. From Table 7, it is shown that 84.2% (202) of the questionnaires were returned for analysis. In establishing the minimum response rate percentage, Mugenda and Mugenda (2003) observed that a 50% response rate is adequate, 60% is good while the response rate of above 70% is very good. Based on this assertion, the current study's response rate of 84.2% is therefore very good. The recorded high response rate can be attributed to the data collection procedures where the researcher pre-notified the participants of the intended and intention of the study, utilised a self-administered questionnaire where the respondents completed the questionnaires and were collected shortly afterward and the researcher made follow up calls to clarify queries as well as prompt the respondents to fill the questionnaires.

4.2.2 Gender of the Respondents

From the exploratory data analysis, the findings of the study show that there was remarkable disparity in terms of number of female staff and their male counterparts, as shown in Table 8.

Table 8: Respondents Gender

	N	Percent	Cumulative Percent
Male	128	63.4	63.4
Female	74	36.6	100.0
Total	202	100.0	

Source: *Survey data (2017)*

From Table 8, it is evident that a significant majority of 128 translating to 63.4% of the respondents were males and only 36.6% of them were females. Although, this finding reveals that a significant majority of people working in Information Technology departments of most of SME in Kenya are males, all gender was represented in the study. This was perceived to enable the study to present findings which are not bias in terms of gender perspectives, opinions and point of view.

4.2.3 Age of the Respondents

Figure 9 presents the summary of the respondents' ages, which was considered important in regard to understanding the concept of SaaS cloud delivery model especially in respect to its fundamental challenges. This was viewed as an important aspect of the study.

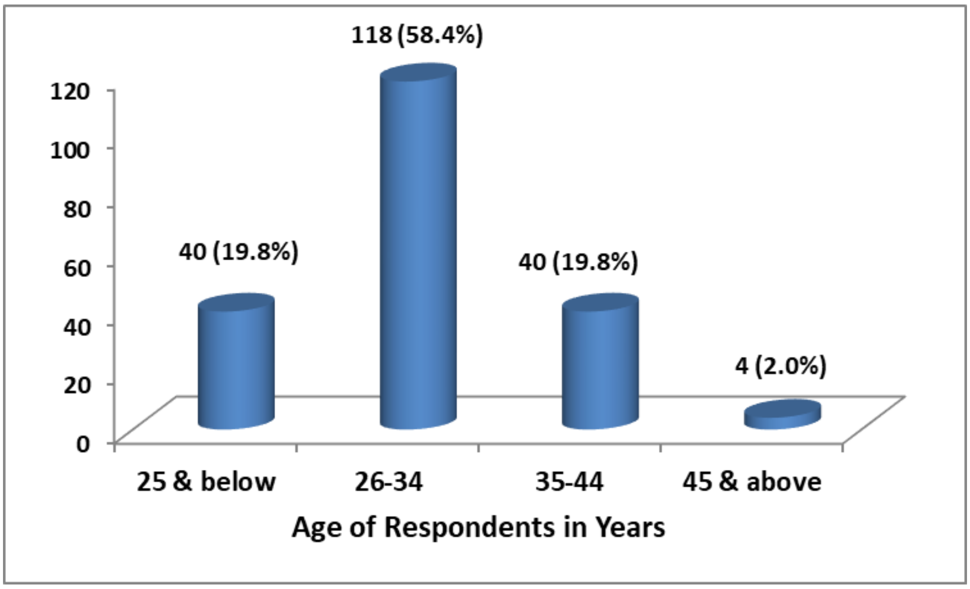


Figure 9: Respondents' Age
Source: *Survey data (2017)*

On the age of the respondents, it is evident from Figure 9 that the majority of the respondents were below 35 years, with 118 (58.4%) of them being in the age bracket of 26 – 34 years and those younger than 25 years of age being 40 (19.8%) of all the IT staff who took part in the study. This finding implies that most of the IT staffs in Kenyans' top 100 SMEs are young people. Only 4 (2.0%) of them were aged 45 years and above. This is not surprising because IT is generally dominated by young people, being viewed as fairly recent technology in comparison to other skills.

4.2.4 Level of Education of the Respondents

The study sought to explore the level of education of IT staff who participated in the study, as shown in Table 9. The knowledge of the level of education of the respondents was considered vital for the study; educational level of the respondents was considered key in understanding of the challenges associated with the implementation of a Security Framework in Software as a Service (SaaS) Cloud Paradigm for SMES.

Table 9: Respondents' Level of Education

	Frequency	Percent	Cumulative Percent
Certificate	2	1.0	1.0
Tertiary	18	8.9	9.9
Degree	146	72.3	82.2
Masters	32	15.8	98.0
Doctorate	4	2.0	100.0
Total	202	100.0	

Source: *Survey data (2017)*

The exploratory data analyses revealed that majority of IT staff in SME organisation were holders of bachelor degrees. This was reflected by the fact that more than seven out of every ten [146 (72.3%)] of the respondents were graduates. The number of those who were holding master's degrees were placed distant second at 15.8%. On the contrary, people with less than degree qualification formed a near negligible proportion of the respondents.

4.2.5 Years Worked in Information Technology / Systems

The study sought to investigate the length of time (years) the respondents had worked in Information Technology/Systems. This was considered as important information for the study, because quality of response was viewed to be dependent on experience in the field of IT. Table 10 shows the summary of the period of time the respondents had worked in the field of IT.

Table 10: Years Respondents worked in Information Technology/Systems

Years	Frequency	Percent	Cumulative Percent
Below 1 Year	10	5.0	5.0
1 to 2 years	80	39.6	44.6
3 to 4 years	48	23.8	68.3
over 5 years	64	31.7	100.0
Total	202	100.0	

Source: *Survey data (2017)*

The findings of the study indicate that majority of the IT staffs who were sampled for the study had experience of more than one year. The results of the survey indicate that the respondents were mainly of 1-2 years and over 5 years of experience as revealed by 80 (39.6%) and 64 (31.7%) of the respondents, respectively. This indicates that significant majority of the respondents had adequate experience to identify challenges experienced in the implementation of a Security Framework in Software as a Service (SaaS) Cloud Paradigm for SMES.

4.2.6 Respondents Role within the Organisation

The study sought to explore the role of the respondents within the SMEs organisations where they were working, as summarised in Table 11.

Table 11: Role of the Respondents in the Organisation

	Frequency	Percent	Cumulative Percent
Director / Owner / CEO	14	6.9	6.9
Finance Controller	12	5.9	12.9
Accounts Personnel	32	15.8	28.7
IT admins / Technicians	94	46.5	75.2
Data User / System User	40	19.8	95.0
Others	10	5.0	100.0
Total	202	100.0	

Source: *Survey data (2017)*

Table 11 reveals that different departments are directly involved with data and participate in decision making of the SMEs in data related issues. However, it emerged that some departments within the organisations received more representation in the study than others. For example, majority of the study participants were IT administrators/Technicians, Accounts personnel and Data User/System Users as reflected by 94 (46.5%), 32 (15.8%) and 40 (19.8%), respectively. Nonetheless, it was evident that all the departments where IT was used were included in the study. This was necessary to create room for generalisation of the results of the study, because views were received from all IT users without bias.

4.2.7 Services Sourced or to be Sourced from Cloud Service Provider

The study sought to investigate the services that the Top 100 SMEs hire or intend to hire from cloud Service Provider, as summarised in Figure 10.

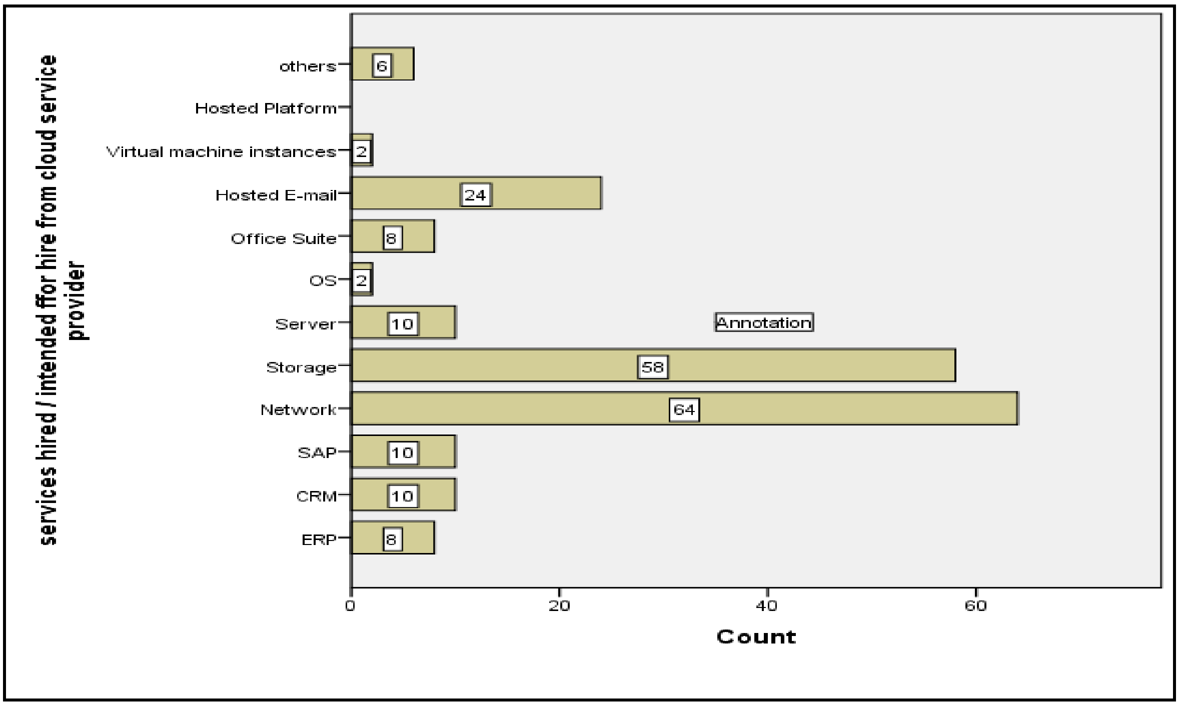


Figure 10: Services Hired from Cloud Service Providers
Source: *Survey data (2017)*

It is evident that network, data storage and hosted e-mail services were most commonly hired services from the cloud service providers.

4.3 Fundamental cloud security challenges experienced by SMEs in Kenya

This objective sought to investigate the fundamental challenges of SaaS cloud delivery model as implemented by selected SMEs in Kenya. It was explored by use of questionnaires whose items were linked to the constructs of security challenges, security measures of cloud computing and concerns to cloud computing.

4.3.1 Security Challenges in Deployment Models

The views of the respondents on security challenges faced in SaaS delivery model in their respective deployment models were collected using eight itemed Likert scaled questionnaire. The items were rated using strongly Agree=5, agree=4, Undecided=3, Disagree=2 and strongly disagree=1. The views of the respondents were summarised in percentage frequencies, as shown in Table 12.

Table 12: Respondents Views of on Security Challenges

Item	SA	A	U	D	SD	M	Std. Dev
Data/information stored on the cloud may face a lot of availability issues due to downtime in the internet.	78 (38.6%)	66 (32.7%)	28 (13.9%)	24 (11.9%)	6 (3.0%)	3.92	1.12
A cloud administrator may become a very high risk if they turn rouge and try and access data stored on clouds.	74 (36.6%)	74 (36.6%)	30 (14.9%)	14 (6.9%)	10 (5.0%)	3.93	1.11
Whenever the data owner makes a command to delete a cloud resource, there is no certain way of telling that the data has been deleted to its entirety.	36 (17.8%)	68 (33.7%)	50 (24.8%)	26 (12.9%)	22 (10.9%)	3.35	1.22
Because the owner of the data has not control over the data handling practices of the cloud vendor, there is no sure way of telling that data is being handled in a lawful way.	56 (27.7%)	58 (28.7%)	42 (20.8%)	38 (18.8%)	8 (4.0%)	3.57	1.19
In SaaS model, hackers can manipulate weakness in data security model to get an illegitimate access to data or application.	44 (21.8%)	76 (37.6%)	48 (23.8%	26 (12.9%)	8 (4.0%)	3.60	1.08
Cloud computing creates lack of liability of providers in case of security incidents.	32 (15.8%)	58 (28.7%)	32 (15.8%)	48 (23.8%)	32 (15.8%)	3.05	1.34
Multi-tenancy in the cloud a major issue for clients due to the possibility of a hacker taking advantage of the same host.	48 (23.8%)	62 (30.7%)	47 (23.3%)	28 (13.9%)	17 (8.4%)	3.49	1.22
Password protection in itself is enough to secure against unauthorised access in the cloud.	32 (15.8%)	58 (28.7%)	21 (10.4%)	56 (27.7%)	35 (17.3%)	2.99	1.37
Mean average response on security challenges						3.49	0.69

SA-strongly agree, A-agree, N-neutral, D-disagree, SD-strongly disagree, M-mean and Std. Dev.-Standard deviation.

Source: *Survey data (2017)*

The findings of the study revealed that Cloud computing face considerable security and related challenges in the implementation of SaaS delivery model. This was reflected by mean average response rate of 3.49 with standard deviation of 0.69, on the rating scale of 1 to 5. All the items were rated above mean score of 2.5; ranging from a minimum of 2.99 to a maximum of 3.93.

This finding affirms the assertion of Shroff (2010) that since cloud computing is not a standalone computing platform because it combines several technologies including networks, operating systems (OS), databases, virtual servers and components, resource scheduling, transaction processing, concurrency control techniques, load balancing, memory management and numerous others for its functionality and operation, a threat in any one of the technologies becomes a threat for the entire cloud platform. This causes a serious security challenge in the implementation of SaaS delivery model.

At a mean response rate of 3.92 (Standard deviation=1.12) a significant majority of 144 translating to 71.3% of the respondents observed that data/information stored on the cloud may face a lot of availability issues due to downtime in the internet. They pointed out that many regions face challenges with stable and affordable internet connections yet all the data, resources and applications are only accessible through the internet. Only 32 (14.9%) of them were on the contrary opinion that cloud face a lot of availability issues due to downtime in the internet.

In support to this finding is Omwansa et al. (2014) whose findings had established that downtime is a major disadvantage of cloud computing especially in evolving countries. They had pointed out that since all the data, resources and applications are only accessible through the internet, an internet outage means users have no access to them.

Similarly, the findings of the study established that a cloud administrator may face a very high risk if they turn rouge and try and access data stored on clouds. This point of view was reflected by a mean average score of 3.93, with nearly three quarters 148 (73.2%) of the IT staff who were engaged in this study agreeing that a cloud administrator may be exposed to high risk if they turn rouge and try and access data stored on clouds.

In addition, it emerged that cloud computing is faced with a lack of certainty in trailing actions of the users. For example, although 50 (24.8%) of respondents remained non-committal, more than a half 104 (51.5%) of them confirmed that whenever the data owner makes a command to delete a cloud resource, there is no certain way of telling that the data has been deleted to its entirety. This means that there is no sure way of confirming that documents or personal data on the cloud has been successfully deleted by the user.

This finding agrees with Behl (2011) who observed that since most cloud platforms are hosted off-site, an organisation is not able to have full control over the hardware, technology and backend details of the cloud platform. Customarily, when an organisation outsources their data and services to a cloud vendor, users are not aware and have no control over the location of their data, which is a serious concern to a user perspective; organisations lose control over their vital data and are not aware of any security mechanisms put in place by the provider.

Equally, Pearson and Benameur (2010) had noted that user-centric control is not possible with the cloud because the vendor acquires full responsibility for storage of data as soon as a SaaS cloud infrastructure is used, hence users lose visibility and control over it. In the cloud archetype, users' data is handled in 'the cloud' on hardware, software and platform the users do not own or control and therefore it becomes a threat in terms of theft.

On the same note, the study revealed that legality of the data in the cloud is not easy to voucher. Majority 114 (56.4%) of respondents, translating to a mean score of 3.57, were of the general feeling that since the owner of the data does not have control over the data handling practices of the cloud vendor, there is no sure way of telling that data is being handled in a lawful way.

The respondents observed that it is not clear that it is possible for a cloud provider to ensure that a data owner can get access to all their data including metadata and system related files. It is also difficult to get data back from the cloud, and avoid vendor lock-in. Equally, nearly six out of ten 120 (59.4%) of the respondents observed that in SaaS model, hackers can manipulate weakness in data security model to get an illegitimate access to data or application.

These findings agree with the position held by Pearson and Benameur (2010) that loss of visibility and control of the data by the consumer in cloud computing may cause risk of misuse, especially for different purposes from those originally notified to and agreed with the consumer, or unauthorised resale.

Similarly, this finding is in line with the argument held by Khan and Malluhi (2010) that data entrusted to different systems and platforms located in different locations, managed by unknown users, and regulated by the laws of other countries cannot be fully be relied on without fear of abuse, loss of confidentiality, integrity and availability of data.

They observe that a consumer does not know whether the security profiles of the remote locations are the same as what they have in-house or whether the regulatory compliances like HIPAA hold in all the locations, does not know who can access the data stored on various disks in multiple locations.

The findings of the study show that multi-tenancy in the cloud is a major issue for clients due to the possibility of a hacker taking advantage of the same host. This was revealed by more than a half 110 (54.5%) of the IT staff who took part in the study and reflected by a mean response rate of 3.49, with a standard deviation of 1.22. The respondents observed that when a multi-tenancy has been achieved, an attacker takes advantage of the system characteristics to hack other users' data. They further argue that the risk from for such attacks is high because they cannot be detected by the hypervisor or the operating system.

This finding concurs with Jahdali et al. (2014) who had postulated that because multi-tenancy in cloud computing is unique in a way that both the attacker and the victim are sharing the same servers, the setup cannot be countered by native security measures and controls because they are not designed to secure inside the servers and they are limited just to the network layer.

Equally, Sen and Sengupta (2005) observed that security challenge is the biggest question that arises to the managements of any organisation that wants to move to the cloud. They reiterate that threats and flaws in technologies like operating systems, virtual platforms, transaction processing systems, and concurrency control procedures and the likes form part of the cloud security issues.

On the contrary, the findings of the study show a sharp division on opinion on whether or not there is lack of liability in case of security incidences as a result of cloud computing. Although, 90 (45.5%) of the respondents held a strong opinion that cloud computing creates lack of liability of providers in case of security incidents, almost equal proportion 80 (39.6%) of the surveyed IT staff refuted the assertion that cloud computing creates lack of liability of providers in case of security incidents.

Similarly, whereas 32 (15.8%) of the respondents strongly believed that password protection in itself is enough to secure against unauthorised access in the cloud, 35 (17.3%) of them held that password protection in itself is not adequate to secure against unauthorised access in the cloud. They claim that some people may misuse existing privileges to gain further access or support third parties in accesses data/information they are not meant to access, this infers with the confidentiality and integrity of information within the cloud service. This finding of the survey is line with the argument by Saripalli and Walters (2010) that by spending a little money to buy cloud space, an attacker has a considerable chance to allocate his VM next to the victim's VM the potential attacker is able to take advantage of the system characteristics to hack breach the victim's data and such attack cannot be easily detected by the hypervisor or the operating system.

4.3.2 Security Measures Provided by Cloud Provider

The study sought to investigate the sufficiency of security measures provided by cloud provider to cater for all the areas of cloud computing that need to be secured. The views of the respondents on sufficiency of security measures were gathered using eight itemed Likert scaled questionnaire.

The constructs of the items were based on possible indicators of security measures towards various areas of cloud computing. The items were to be rated using 5=Very sufficient, 4=largely sufficient, 3=Somehow sufficient, 2=largely insufficient and 1=Very insufficient. The views of the respondents were summarised in percentage frequencies, as shown in Table 13.

Table 13: Views of Respondents on Security Measures

Item	5	4	3	2	1	Mean	Std Dev.
Cloud computing supplier maintains proper security monitoring logs of all access to your data and documents access as routine, random audit, or suspicious leveraging their prescribed scripts and operational procedures as the basis for all audit in all deployment models.	74 (36.6%)	72 (35.6%)	40 (19.8%)	10 (5.0%)	6 (3.0%)	3.98	1.01
User access control rules, security policies and enforcement are made available to the customer in a well-informed manner.	76 (37.6%)	102 (50.5%)	18 (8.9%)	6 (3.0%)	0 (0.0%)	4.23	0.73
In SaaS, applications are multi-tenant hosted by 3rd party usually exposes functionality could result multifaceted security issues.	48 (23.8%)	84 (41.6%)	50 (24.8%)	14 (6.9%)	6 (3.0%)	3.76	0.99
Cloud computing providers provide sufficient security for data at rest. (Stored data in the cloud).	50 (24.8%)	80 (39.6%)	44 (21.8%)	22 (10.9%)	6 (3.0%)	3.72	1.04
Cloud computing providers provide sufficient security for data in transit. (Data being transferred from the cloud to the user computers and vice versa).	46 (22.8%)	76 (37.6%)	58 (28.7%)	20 (9.9%)	2 (1.0%)	3.71	0.96
Cloud computing providers provide sufficient authentication platform for users to access the cloud.	38 (18.8%)	96 (47.5%)	52 (25.7%)	10 (5.0%)	6 (3.0%)	3.74	0.92
Cloud providers have sufficient and credible policies and practices especially for things like data retention, deletion and security.	40 (19.8%)	82 (40.6%)	48 (23.8%)	28 (13.9%)	4 (2.0%)	3.62	1.01
Customers understand how incidents and disasters will affect their data and therefore have relevant recovery procedures for the same.	24 (11.9%)	54 (26.7%)	60 (29.7%)	36 (17.8%)	28 (13.9%)	3.05	1.21
Mean average response rate on sufficiency of security measures						3.73	0.98

5-Very sufficient; 4-Largely sufficient; 3-somehow sufficient; 2-largely insufficient; 1-very insufficient; M-mean and Std. Dev.-Standard deviation

Source: *Survey data (2017)*

Table 13 indicates that members that were directly involved with the data and decision making of the SME who took part in the survey rated, as largely sufficient (average score=3.73; standard deviation=0.98), in the scale of 1 to 5 of sufficiency of security measures provided by cloud providers to cater for most of the areas of cloud computing that need to be secured.

All the indicators were rated above 3.00, with “user access control rules, security policies and enforcement” receiving the highest rating (mean average score=4.23; standard deviation=.73). Nearly nine out of ten 176 (88.1%) of the respondents held a general feeling that user access control rules, security policies and enforcement are made available by the cloud providers to the customer in a well-informed manner. Sen and Sengupta (2005) had observed that cloud technologies be secure enough to provide for overall security of the system; the network between the end users and the cloud infrastructure needs to be secure, data at rest also needs to be secure by encrypting the data and enforcing relevant policies for data sharing and resource distribution and memory management systems need to be secured.

Similarly, although some 32 (15.9%) of the respondents held a contrary opinion, majority 122 (60.4%) of them observed that cloud providers have sufficient and credible policies and practices especially for things like data retention, deletion and security. Those who held contrary opinion argue that policies and practices on issues like data retention, deletion and security are insufficient and not adequate to address security challenges. They felt that some customers hardly ever have their legal and regulatory experts inspect cloud provider policies and practices data retention, deletion and security.

It emerged that more than seven out of every ten 146 (72.3%) of the SMEs staff sampled for the survey, reflecting a mean average score of 3.98 (standard deviation=1.01), were in agreement that cloud suppliers maintain proper security monitoring logs of all access to their data and documents access as routine, random audit, or suspicious leveraging their prescribed scripts and operational procedures as the basis for all audit in all deployment models.

However, some 16 (8.0%) of them said cloud computing suppliers do not sufficiently maintains proper security monitoring logs of all access to their data and documents access as routine, random audit, or suspicious leveraging their prescribed scripts and operational procedures as the basis for all audit in all deployment models. They also observed that some cloud vendors also usually do not allow clients to carry out audits, meaning that certain kind of compliances cannot be achieved.

On multi-tenant, the findings of the study show that although a sizeable proportion 50 (24.8%) of the respondents remained non-committal, many 132 (65.3%) of them were in agreement that in SaaS, applications that are multi-tenant hosted by 3rd party usually expose functionality that could result in to multifaceted security issues. Likewise, despite the fact that 78 (38.6%) of the sampled staff of SMEs agree that customers of cloud computing understand how incidents and disasters affect their data, 64 (31.7%) of them alluded that cloud computing suppliers lack relevant recovery procedures for such data. This was reflected by a mean average score of 3.05, with standard deviation of 1.21.

On the sufficiency of security measure on data, many 130 (64.4%) of the study participants were contented that cloud computing providers provide moderately sufficient security for data at rest/ stored data in the cloud, translating to a response rate of 3.72 (std. dev.=1.04). On the other hand, some 28 (13.9%) of the respondents believed that there is insufficient security of such data, while 44 translating to more than a fifth (21.8%) of respondents also remained doubtful on the security of data in the cloud.

Equally, it came out clearly that despite the fact that a majority of 122 (60.4%) of the sampled staff were of the general agreement that cloud computing providers provide sufficient security for data in transit, about a tenth 22 (10.9%) of them insisted that the providers do not provide sufficient security for the data being transferred from the cloud to the user computers and vice versa. Interestingly, more than one out of every four 58 (28.7%) of those who were directly involved with the data and decision making of the SME who took part in the survey were not aware of security concerns of data in transit and how the cloud computing providers handle the matter.

This was despite the fact that CPNI Security Briefing (2010) had pointed out that cloud vendors should come up with different technologies and standards to increase their security but then the customers to ensure that security in the cloud meets their own security requirements and policies. They suggest that both vendors and users should carry out risk assessments and due diligence of the cloud security models.

The results of the survey also revealed that there was differing opinion from the staff directly involved with the data and decision making of the SME on provision of authentication platform. This was revealed by the fact that whereas, 38 (18.8%) of the staff sampled for the survey strongly believed that cloud computing providers provide sufficient authentication platform for users to access the cloud, some 16 (8.0%) of them held a contrary opinion.

These respondents believe that cloud providers sometimes do not provide users with strong user access control to access data so as to keep off unwanted users. However, 52 (25.7%) of the respondents said that although there is some authentication platform for users to access the cloud, it is only somehow sufficient.

4.3.3 Concerns in Cloud Computing in Deployment Models

The views of the respondents on concerns on cloud computing in SaaS deployment models were gathered from members that were directly involved with the data and decision making in the SME. Their views were gathered using eight itemed Likert scaled questionnaire on the main concerns in their approach to cloud computing. The items were to be rated using: Not Important at all=1; Slightly Important=2; Somewhat Important=3; Largely Important=4 and Very Important=5. The views of the respondents were summarised in percentage frequencies, as shown in Table 14.

Table 14: Views of the Respondents on Concerns on Cloud Computing

Item	1	2	3	4	5	M	Std Dev.
Privacy	24 (11.9%)	14 (6.9%)	4 (2.0%)	24 (11.9%)	136 (67.3%)	4.16	1.42
Availability of services and/or data	18 (8.9%)	16 (7.9%)	8 (4.0%)	32 (15.8%)	128 (63.4%)	4.17	1.33
Integrity of services and/or data	16 (7.9%)	16 (7.9%)	8 (4.0%)	24 (11.9%)	138 (68.3%)	4.25	1.30
Confidentiality of corporate data	24 (11.9%)	8 (4.0%)	6 (3.0%)	34 (16.8%)	130 (64.4%)	4.18	1.37
Loss of control of services and/or data	14 (6.9%)	20 (9.9%)	12 (5.9%)	58 (28.7%)	98 (48.5%)	4.02	1.25
Lack of liability of providers in case of security incidents	14 (6.9%)	24 (11.9%	30 (14.9%)	60 (29.7%)	74 (36.6%)	3.77	1.25
Inconsistency between trans national laws and regulations	18 (6.9%)	22 (11.9%	40 (14.9%)	56 (29.7%)	66 (36.6%)	3.64	1.28
Intra-clouds (vendor lock-in) migration	14 (6.9%)	26 (11.9%	30 (14.9%)	68 (29.7%)	64 (36.6%)	3.70	1.23
Mean average score on concerns on cloud computing						3.99	1.30

1=Not Important at all; 2=Slightly Important; 3=Somewhat Important; 4=Largely Important; 5=Very Important; M=mean score and Std. Dev.= Standard Deviation.

Source: *Survey data (2017)*

Table 14 reveals that people directly involve in data and decision making in the top 100 SMEs organisations in Kenya generally feel that concerns on cloud computing are largely important. This was reflected by a mean average score of 3.99 (standard deviation=1.30), with most of the concerns rated as very important (mean score rating > 4.00). Concern on integrity of services and/or data received the highest rating (mean=4.25), with over four fifth 162 (80.2%) of the respondents indicating that concern on integrity of services or data is quite important in regard to cloud computing.

Stallings and Brown (2008) had observed that cloud computing provider is entrusted by their clients to provide integrity for their data but due to the working nature of the cloud model, several threats including complicated insider attacks can take place. Malicious employee can intentionally fabricate a program to fail when a certain command is executed or a certain time is reached. Moreover, the security of cloud services is reliant on the security of the API or interfaces that the cloud providers offer to their customers, thus if unauthorised users gain control of interfaces, data integrity can be seriously violated.

Equally, concerns on privacy was rated very high, as reflected by a mean rating score of 4.16 (standard deviation =1.42) with a significant majority 160 (79.2%) of the respondents asserting that privacy of data and services in quite important in cloud computing. In addition, the findings of the study show that confidentiality of corporate data is very important (mean score = 4.18) and key in cloud computing, with nearly two thirds 130 (64.4%) of rating it as of very high importance.

This finding concurs with the views held by Modi, Patel, Borisaniya, Patel and Rajarajan (2013) that unauthorised right of entry may take place due to an application vulnerability or weak identification, increasing chances of confidentiality and privacy breaches. However, they asserted that the cloud provider is responsible for providing secure cloud instances, which should ensure users privacy. Similarly, Zissis and Lekkas (2012) portends that because the cloud allows many access points for its users to connect (usually from anywhere with internet access), authorisation is crucial to maintain data integrity and security at large.

It was established that a significant majority of 160 translating to 79.2% of the respondents were in general agreement that availability of services and/or data in cloud computing is of a very important concern (mean score=4.17) to the users. On the same note, it emerged that loss of control of services and/or data is equally another important concern in cloud computing. This was revealed by nearly a half 98 (48.5%) of study participants who strongly observed that since most cloud platforms are hosted off-site, their organisation does not have full control over the hardware and technology. In addition, most of the study participants held that since cloud computing involve outsourcing of data and services to a cloud vendor, the users are not aware and have no control over the location of their data, which is a very serious concern, as reflected by a mean score of 4.02.

On the flip flop, the study findings revealed that although issues of security incidents are a concern to many 134 (66.3%) users of cloud computing, a considerable proportion 38 (18.8%) of the respondents observed that issues of security incidents are not a serious concern. However, majority of the respondents held that there is lack of liability of providers in case of security incidents. Some of the respondents were concerned that customers are sometimes never made to understand how incidents and disasters affect their data.

However, the findings of the study established that although there is concern about inconsistency between transnational laws and regulations, it is not very serious as reflected by a mean score of 3.64 (standard deviation=1.28). Equally, intra-clouds (vendor lock-in) migration generates relatively low concern rate (mean score = 3.70) among the users/potential users of cloud computing services, with some 40 (18.8%) of the respondents disagreeing with assertion that intra-clouds migration is a cause of concern in the cloud computing model.

Further, the data on concerns on cloud computing was tested using a Chi-squared test. The chi-squared test was used to determine whether there are significant concerns on cloud computing. This was done by using chi-square test whether the eight concerns raised by the top 100 SMEs organisations in Kenya are statistically significant. Response frequencies were grouped and summed in five levels, from strongly disagree to strongly agree, separately for the seven concerns raised. The data met the assumptions of independence and identical distribution of variables with none of the expected frequencies being less than 5. The Chi-square tests results are shown in Table 15.

Table 15: Chi-Square Test Results on Concerns on Cloud Computing

Item	n	χ^2 value	Asymp. Sig.	df	Conclusion
Privacy	202	89.188	.000	4	Significant
Availability of services and/or data	202	46.515	.000	4	Significant
Integrity of services and/or data	202	4.287	.369	4	Not significant
Confidentiality of corporate data	202	48.347	.000	4	Significant
Loss of control of services and/or data	202	13.149	.011	4	Significant
Lack of liability of providers in case of security incidents	202	15.871	.003	4	Significant
Inconsistency between trans national laws and regulations	202	6.020	.198	4	Not Significant
Intra-clouds (vendor lock-in) migration	202	11.267	.024	4	Significant

The results in Table 15, shows that most of the concerns raised by the top 100 SMEs organisations in Kenya are statistically significant, p< .05, with those who agreed and strongly agreed that the concerns raised are serious forming majority of the respondents. Only two of the concerns did not meet statistical significance. For example, concern on the integrity of services and/or data [n= 202; χ^2 (4) = 4.287, p=.369] and inconsistency between Trans national laws and regulations [n= 202; χ^2 (4) =6.020, p=.198] were not significant.

4.4 Investigate the Security Challenges of the Cloud

This objective sought to investigate how data stored on the cloud reacts during different file operations and well as determine the threats posed in cloud from the provider's end. This was experimented by use of OwnCloud version 10.0.4.

OwnCloud was installed on a domain that the researcher registered and hosted online. Accounts were then created on the software that were given to different users to save their dummy data in using both the OwnCloud client software version 2.4.0 as well as the web browser. The steps for the installation are described in details in the section below:

To start the installation, OwnCloud’s release key was downloaded using the curl command and imported with the apt-key utility with the add command as shown below:

```
sudo                                                                                  curl
https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04/Release.key       |
sudo apt-key add –
```

This yielded an output as follows:

```
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left  Speed
100  1358  100  1358    0     0  2057         0      --:--:-- --:--:--  --:--:--  2057
OK
```

The 'Release.key' file contains a PGP (Pretty Good Privacy) public key which is usually used to verify that the OwnCloud package is authentic.

In addition to importing the key, a file called owncloud.list in the sources.list.d directory was created. The file contains the address to the OwnCloud repository. This was done by the following command:

```
echo  'deb  https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04/  /'  |
sudo tee /etc /apt/sources.list.d/owncloud.list
```

After adding a new source, the apt-get utility was used and the update command to make apt aware of the change by issuing the following command:

```
sudo apt-get update
```

Finally, the installation of OwnCloud was performed using the apt-get utility and the install command:

```
sudo apt-get install owncloud
```

After completing the OwnCloud server installation, the database was configured for it to be used. To get started, this was done by logging into MySQL with the administrative account with the command as shown below:

```
mysql -u root -p
```

OwnCloud requires a separate database for storing administrative data which was named as owncloud as shown below:

```
CREATE DATABASE owncloud;
```

Thereafter, a separate MySQL user account was created that interacts with the newly created database by issuing the following command:

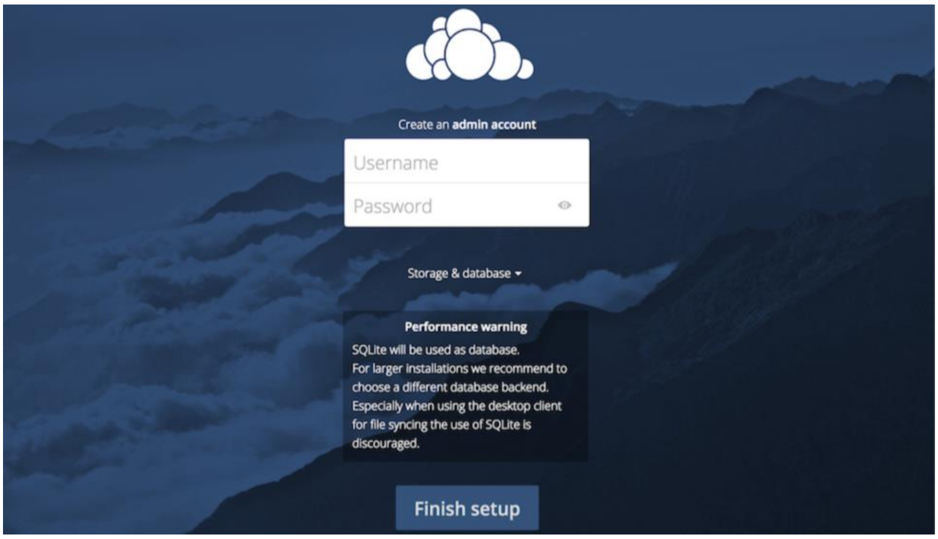
```
GRANT ALL ON owncloud.* to 'owncloud'@'localhost' IDENTIFIED BY ‘password’;
```

With the user assigned access to the database, perform the flush-privileges operation to ensure that the running instance of MySQL knows about the recent privilege assignment by issuing the following command:

```
mysql> FLUSH PRIVILEGES;
```

This concludes the configuration of MySQL. The OwnCloud web interface can be accessed through a web browser through a domain that was purchased separately by opening the address https://rupra.co.ke/owncloud.

This brings up a screen as shown in Figure 11:



Performance warning

SQLite will be used as database.
For larger installations we recommend to choose a different database backend.
Especially when using the desktop client for file syncing the use of SQLite is discouraged.

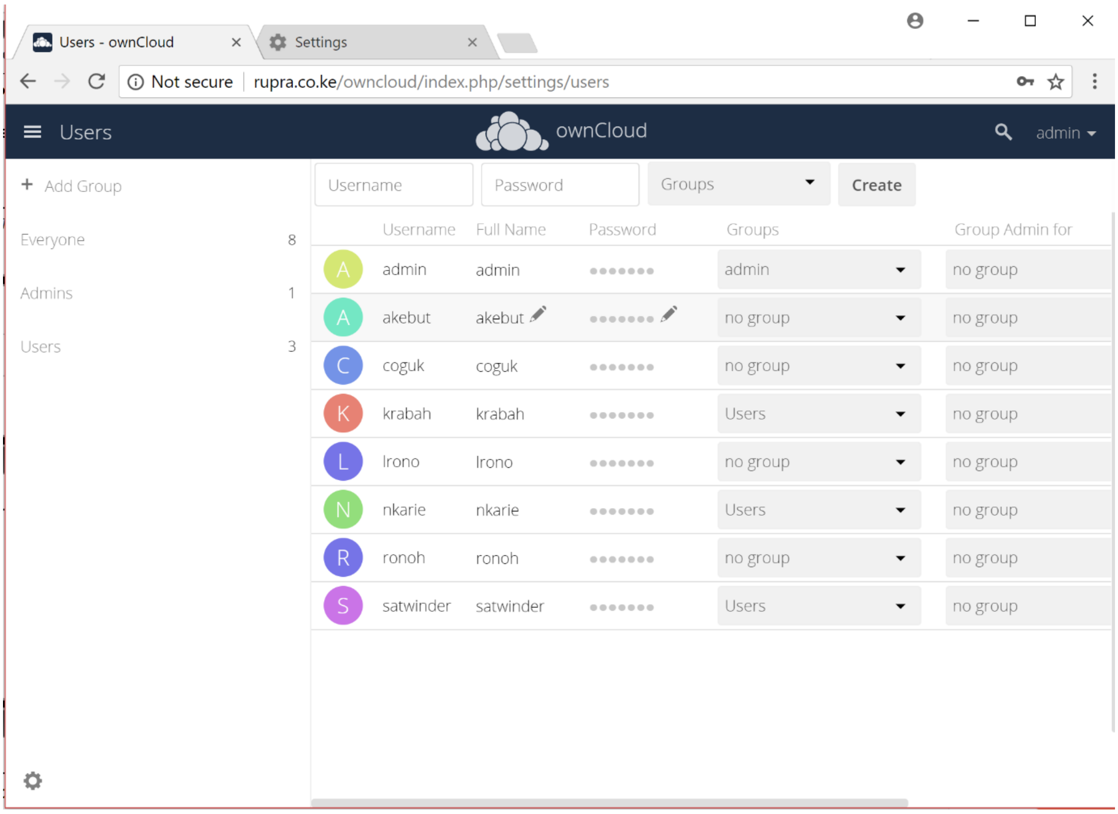
Figure 11: OwnCloud Setup
Source: *Experimental Data*

Finally, the database information that was configured in the previous step was entered to complete the setup and to sign into OwnCloud.

4.4.1 The Challenge of Insider Threat

This is the worst-case scenario for when a malicious system administrator or employee works for the cloud provider. Because of their business role in the cloud provider, the insider can use their authorised user rights to access sensitive data. In fact, Jansen (2011) had noted that an internal attacker is commonly an employee of the cloud vendor, the cloud customer or other third-party provider organisation supporting the operation of a cloud service, hence, they may have existing authorised access to cloud services and customer data or supporting infrastructure and applications. Equally, Sen (2013) had established that internal attackers may use existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within the cloud service. Depending on the insider's motives, the result of such an attack in a cloud infrastructure will vary from data leakage to severe corruption of the affected systems and data. This concurs with the observation made by Mather et al. (2009) that cloud computing is a fairly recent technology in comparison to other technologies in the computing timeline, hence there are no many common and industry accepted cloud security standards, posing additional challenges for users and companies

It is noted using OwnCloud that as much as the administrator does not have access to user passwords, they have the ability to change the password for any user at any given time.



Everyone	8
Admins	1
Users	3

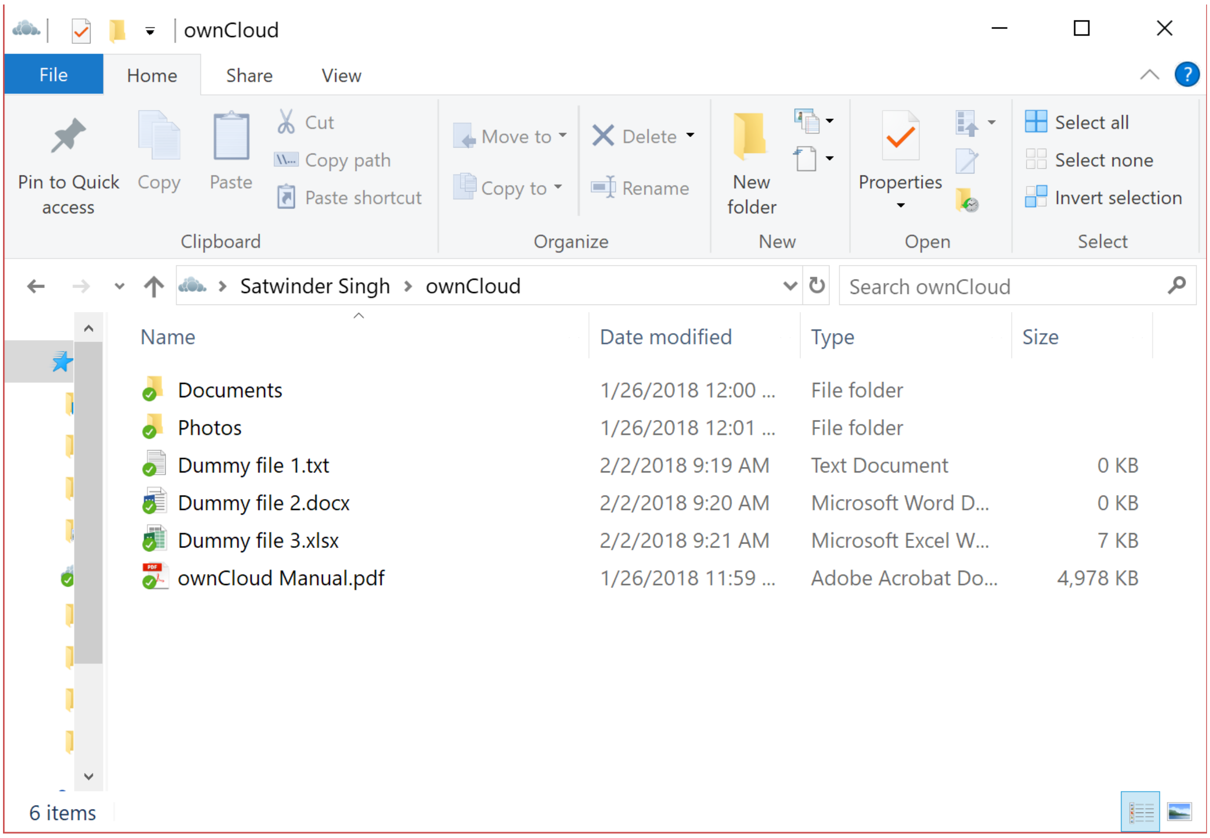
Username	Full Name	Password	Groups	Group Admin for
admin	admin	●●●●●●●	admin	no group
akebut	akebut	●●●●●●●	no group	no group
coguk	coguk	●●●●●●●	no group	no group
krabah	krabah	●●●●●●●	Users	no group
lrono	lrono	●●●●●●●	no group	no group
nkarie	nkarie	●●●●●●●	Users	no group
ronoh	ronoh	●●●●●●●	no group	no group
satwinder	satwinder	●●●●●●●	Users	no group

Figure 12: Users List and Password change
Source: *Experimental data (2017)*

Once the password for any user is changed, the insider can easily log in to the account of the user and therefore gain access to their data and causing confidentiality, integrity and availability compromise.

4.4.2 Challenge of Deleted Data

Dummy files were saved on the cloud using the desktop utility shown below. These files were deleted from the desktop utility moments later. They certainly cease to exist on the local computer after deletion.

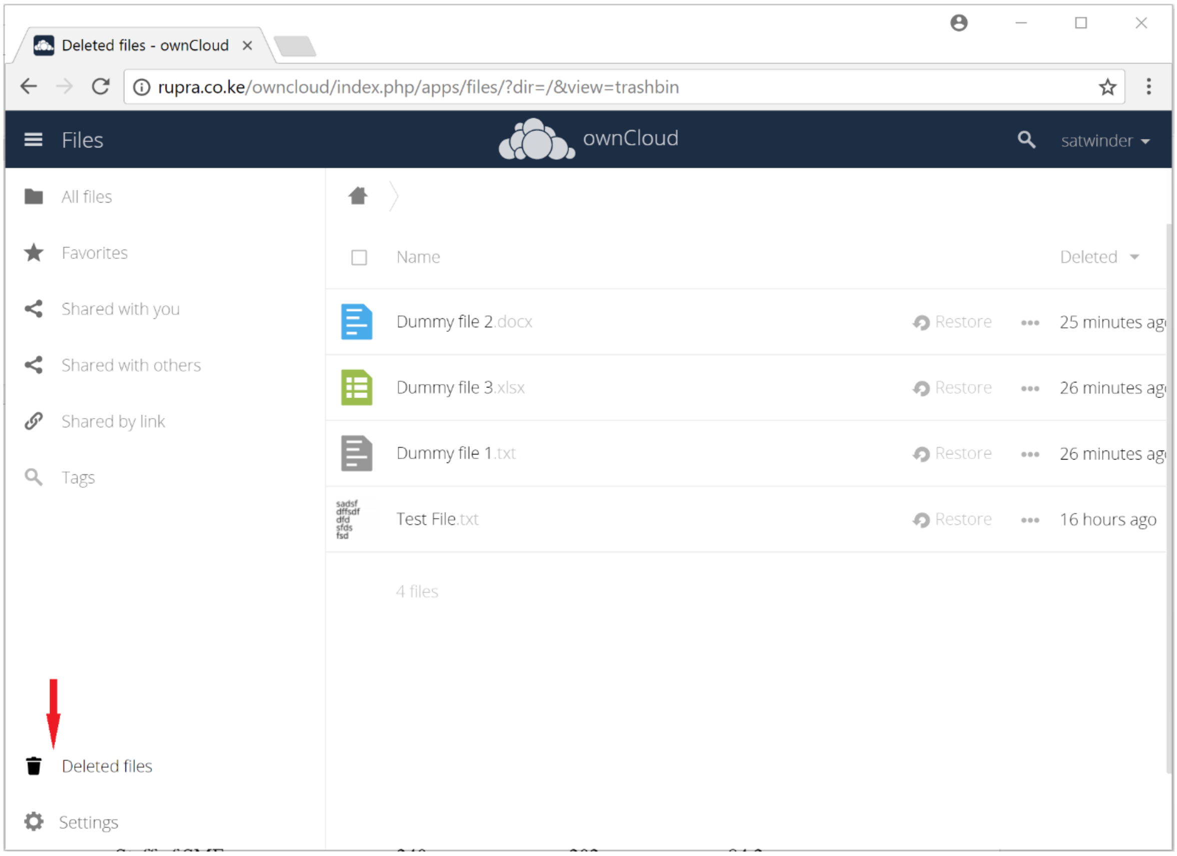


Name	Date modified	Type	Size
Documents	1/26/2018 12:00 ...	File folder	
Photos	1/26/2018 12:01 ...	File folder	
Dummy file 1.txt	2/2/2018 9:19 AM	Text Document	0 KB
Dummy file 2.docx	2/2/2018 9:20 AM	Microsoft Word D...	0 KB
Dummy file 3.xlsx	2/2/2018 9:21 AM	Microsoft Excel W...	7 KB
ownCloud Manual.pdf	1/26/2018 11:59 ...	Adobe Acrobat Do...	4,978 KB

Figure 13: Files Stored in the Cloud
Source: *Experimental data (2017)*

However, these files still remained in the cloud for an additional 180 days. These files are not permanently deleted until you manually delete them, or when your cloud storage is full and the files are automatically deleted to make room for new ones.

The deleted files do not show in the desktop of the client anymore nor do they show in the web directories; however they still stay in the deleted files section as shown in Figure 14.



rupra.co.ke/owncloud/index.php/apps/files/?dir=/&view=trashbin

☐ Name			Deleted
Dummy file 2.docx	Restore	•••	25 minutes ag
Dummy file 3.xlsx	Restore	•••	26 minutes ag
Dummy file 1.txt	Restore	•••	26 minutes ag
Test File.txt	Restore	•••	16 hours ago

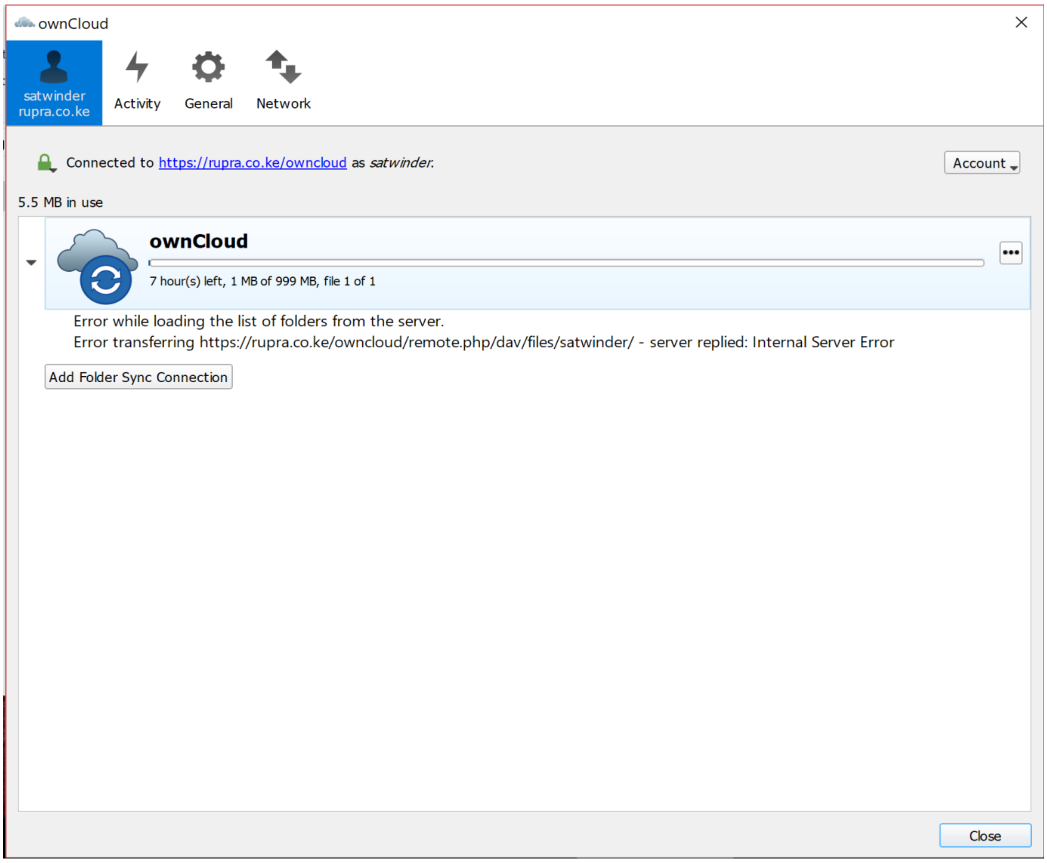
4 files

Figure 14: Deleted Documents in the Cloud
Source: *Experimental data (2017)*

Similarly, Dropbox, One Drive and Google and many other cloud types keep versions of deleted files for up to 30 days as stated in their documentation. This fact is corroborated by assertions of Romanosky (2016) that cloud computing challenges that confront SMEs in Kenya include personnel security due to cloud policy issues and improper data deletion in the cloud.

4.4.3 Challenge of Bandwidth and Availability

Uploading and synchronising data on the cloud requires a stable type of internet connection. One GB of data is uploaded through the client utility took approximately 7 hours with a 2Mbps shared Safaricom connection as shown in Figure 15. Other normal operations were also taking place using the same internet. This may not be a problem for uploading a few files, however if a firm is planning to shift their entire or partial infrastructure on the cloud, then a reliable and stable internet connection is mandatory.



Connected to https://rupra.co.ke/owncloud as *satwinder.*

5.5 MB in use

ownCloud

7 hour(s) left, 1 MB of 999 MB, file 1 of 1

Error while loading the list of folders from the server.
Error transferring https://rupra.co.ke/owncloud/remote.php/dav/files/satwinder/ - server replied: Internal Server Error

Figure 15: Cloud data upload rates
Source: *Experimental data (2017)*

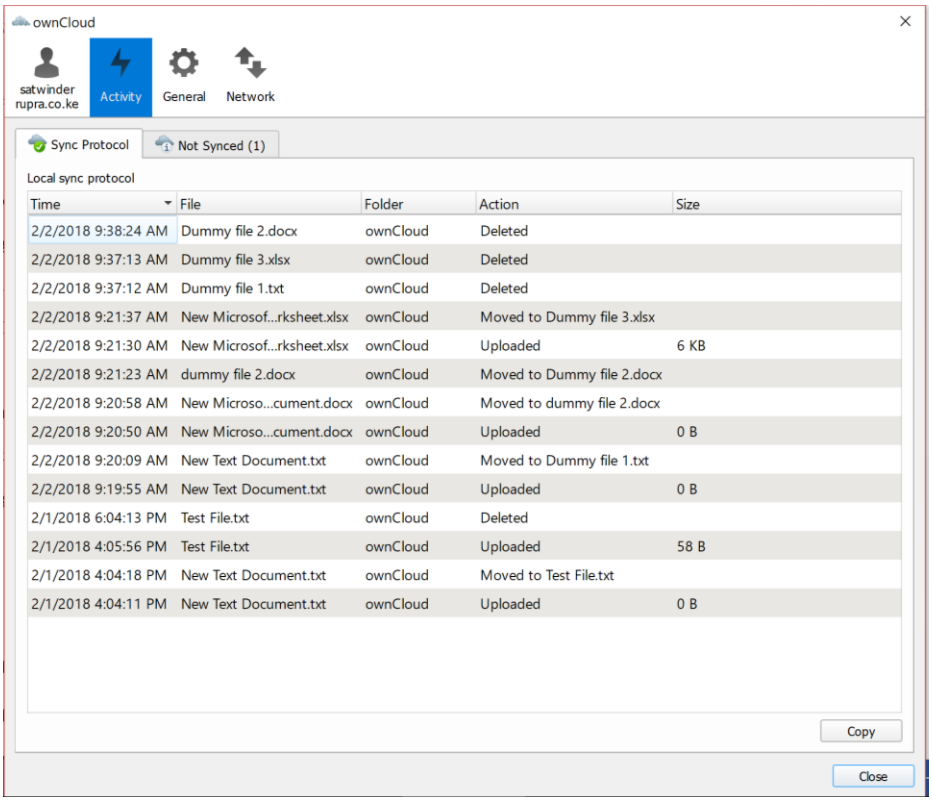
A 10mbps speed would be optimum as well as a failover link in case the primary one is down. Otherwise an SLA agreement of a 99.5% or above by the ISP is required which translates to about 1.8 days in a year. Likewise, a similar SLA with the cloud provider is mandatory although during the experiment, there was no downtime noted over a period of three months showing stability on the cloud provider's side.

Also attacks on identity services or network connectivity, such as DDoS attacks can jeopardise the availability or degrade the performance of the service. Saripalli and Walters (2010) had pointed out that cloud computing faces additional set of challenges including downtime: Many parts of Kenya still face challenges with stable and affordable internet connections. They observe that all the data, resources and applications are only accessible through the internet; an internet outage means users have no access to them.

4.4.4 Challenge of Non-Repudiation

It is always challenging to ensure true non-repudiation and shifting the data to cloud may make this even more difficult due to login from multiple systems (smartphone, desktop/laptop) or access from devices which do not have a static IP.

OwnCloud shows a number of activities that are carried out on the cloud as shown in Figure 16:



Local sync protocol

Time	File	Folder	Action	Size
2/2/2018 9:38:24 AM	Dummy file 2.docx	ownCloud	Deleted	
2/2/2018 9:37:13 AM	Dummy file 3.xlsx	ownCloud	Deleted	
2/2/2018 9:37:12 AM	Dummy file 1.txt	ownCloud	Deleted	
2/2/2018 9:21:37 AM	New Microsof...rksheet.xlsx	ownCloud	Moved to Dummy file 3.xlsx	
2/2/2018 9:21:30 AM	New Microsof...rksheet.xlsx	ownCloud	Uploaded	6 KB
2/2/2018 9:21:23 AM	dummy file 2.docx	ownCloud	Moved to Dummy file 2.docx	
2/2/2018 9:20:58 AM	New Microso...cument.docx	ownCloud	Moved to dummy file 2.docx	
2/2/2018 9:20:50 AM	New Microso...cument.docx	ownCloud	Uploaded	0 B
2/2/2018 9:20:09 AM	New Text Document.txt	ownCloud	Moved to Dummy file 1.txt	
2/2/2018 9:19:55 AM	New Text Document.txt	ownCloud	Uploaded	0 B
2/1/2018 6:04:13 PM	Test File.txt	ownCloud	Deleted	
2/1/2018 4:05:56 PM	Test File.txt	ownCloud	Uploaded	58 B
2/1/2018 4:04:18 PM	New Text Document.txt	ownCloud	Moved to Test File.txt	
2/1/2018 4:04:11 PM	New Text Document.txt	ownCloud	Uploaded	0 B

Figure 16: Cloud Activities Log
Source: *Survey data (2017)*

This may still pose a challenge of non-repudiation because when a dynamic IP is used to connect to the cloud (which is mostly the case with mobile data), not much information will be logged to hold a user accountable for some operations. This could eventually lead to a user denying their actions unless some other form of authentication is able to prove that a user logging in and carried out some functions. This assertion concurs with the point of view held by Feng et al. (2010) that the requirement of evidence can guarantee the non-repudiation and not all users or service providers are willing to completely obey the rules set by the protocol. In most cases the honest party will suffer the unfairness if there is no mechanism to protect them.

4.4.5 Foreign Law Issues and Government Regulations

In traditional IT data and processes remain on-premises, so foreign jurisdictions are usually not an issue. Cloud services sometimes involves the use of cloud providers or datacentres abroad, which means that to a certain extent, foreign jurisdictions may have an impact on the security and privacy of the cloud service. For example, violations of the law by the other customers (co-tenants) may lead to services being ordered shut (for example as part of a criminal prosecution), without taking proper care of the other customers. It has been argued by legal experts that even if the physical location of supporting equipment or data centres are not in a foreign country there could still be an impact. In this regard, Wahlgren and Kowalski (2013) had argued that cloud customers may be able to access their data and service irrespective of the geographical location, implying that the cloud user has no control or whereabouts of the location of the assets and cloud vendor does not have restrictions over the location of its users.

However, according to the Kenyan law, a person who knowingly and without authority discloses any password, access code or other means of gaining access to any program or data held in any computer system commits an offence and is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment term for a term not exceeding three years, or to both. In the event that a user is unknowingly duped into disclosing a password to a malicious user, he or she may still be held liable for a crime and prosecuted. Therefore, it is of utmost important to understand the cyber laws carefully and SMEs should understand which foreign jurisdictions may play a role for data stored in different countries and if there are incompatibilities with Kenyan laws (Kenya Gazette Supplement, 2017).

4.4.6 Hacking Issues Due to Network, API or Social Weaknesses

Cloud computing services are consumed and managed via internet connections. Therefore, like any other online service, SMEs need to be aware of the risk of network attacks like spoofing websites, sniffing/eavesdropping network traffic, Denial-of-Service attacks, man-in-the-middle attacks, pharming, wiretapping, etc., on the normal end-user interfaces, as well management/administrator interfaces, application programming interfaces (APIs), web-services. Sengupta et al. (2011) in their discussion of security issues in a cloud computing environment focused on technical security issues arising from the usage of cloud services. They observed that security threats presented in the cloud include VM-Level attacks, isolation failure, management interface compromise and compliance risks and their mitigation.

As a result of the findings highlighted in this chapter, it is well noted that cloud computing has several challenges, threats and vulnerabilities that need to be addressed for SME users to benefit from the technology. The bottom line for the cloud security framework is to achieve information security (confidentiality, integrity and availability) as is the case with all IT systems.

The challenges highlighted in chapter four experimental analyses can be summed up as below:

i. Insider threats are a big risk to the usage of data in the cloud.
ii. Deleted data storage can cause numerous security challenges if placed in the wrong hands.
iii. Bandwidth and cloud provider availability need to be addressed.
iv. Challenge of repudiation leading to a user denying their actions.

The major challenges highlighted in chapter four by the SMEs feedback can be summed up as below:

i. Data/information stored on the cloud may face a lot of availability issues due to downtime in the internet.
ii. A cloud administrator may become a very high risk if they turn rouge and try and access data stored on clouds.
iii. Because the owner of the data has not control over the data handling practices of the cloud vendor, there is no sure way of telling that data is being handled in a lawful way. His translates into loss of control over the data stored in the cloud.
iv. In SaaS model, hackers can manipulate weakness in data security model to get an illegitimate access to data or application.
v. Multi-tenancy in the cloud a major issue for clients due to the possibility of a hacker taking advantage of the same host.

Similarly, as suggested in the last section of the findings in this chapter, Privacy, Availability of services and/or data, Integrity of services and/or data, Confidentiality of corporate data and

Loss of control of services and/or data came out as the main concerns by the SMEs as they approach to Cloud Computing.

4.5 Developed Framework

From the previous studies, the critical review and the results of the data collection, it is clear that security is a major concern when SMEs 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 total system security. As organisations plan and transfer their applications and data to the cloud, it is critical that the level of security provided in the cloud paradigm be equal if not better than those provided by in-house IT infrastructures.

The framework developed by the researcher is as indicated in the Figure 17. The author proposes an eight-stage cloud security framework divided in two sections. The first five stages are Identify, Protect, Detect, Respond and Recover. The second section includes Metric Hierarchy, Index of Security and finally Implementation of a Secure Cloud.

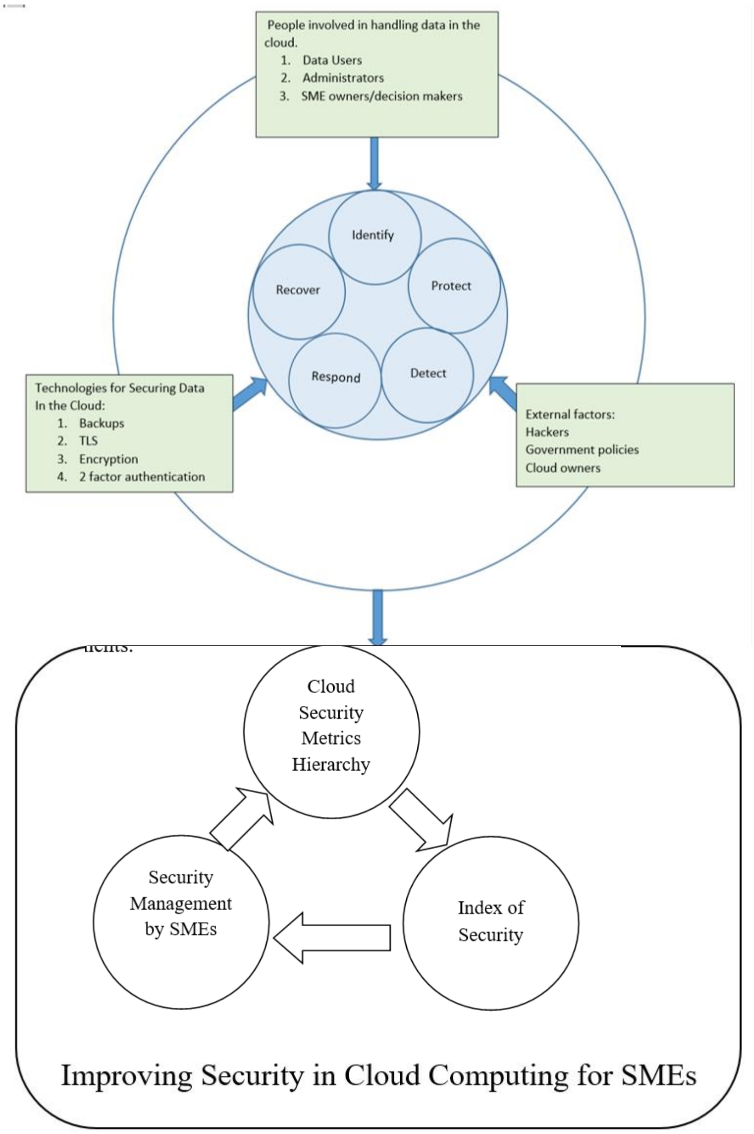

People involved in handling data in the cloud.
1. Data Users
2. Administrators
3. SME owners/decision makers
Identify
Recover
Protect
Respond
Detect
Technologies for Securing Data In the Cloud:
1. Backups
2. TLS
3. Encryption
4. 2 factor authentication
External factors:
Hackers
Government policies
Cloud owners
Cloud Security Metrics Hierarchy
Security Management by SMEs
Index of Security
Improving Security in Cloud Computing for SMEs

Figure 17: Framework for Improving Security in Cloud Computing
Source: *Author* (2019)

The developed framework has considered 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 SMEs need a cloud security framework with the ability to guide them on the three core factors that cause compromise on security (people, lack of technologies and external factors). 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.

4.5.1 Components of the Framework

This section provides an overview of the framework levels that an SME can leverage to align with the core to achieve security in the cloud. Table 16 shows how the framework components are subdivided into areas of security that needs to be addressed.

Table 16: Framework Component Subdivision

Identify	Protect	Detect	Respond	Recover
Asset management	Access Control	Anomalies and Events	Response planning	Recovery Planning
Business environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Mitigation	Communications
Risk Assessment	Information Protection Processes and Procedures		Improvements	
Risk Assessment Strategy	Maintenance		Analysis	
Supply Chain Risk Management	Protective Technology			

Source: *Framework (2019)*

The SMEs are responsible for identifying and managing IT assets as this is the first step in effective IT governance and security, and yet has been one of the most challenging. According to the Centre for Internet Security (CIS) asset inventory is the first priority in setting up any secure computing infrastructure. However, an accurate IT inventory, both of physical assets and logical assets, has been difficult to achieve and maintain for organisations of all sizes and resources.

Inventory solutions are limited in being able to identify and report on all IT assets across the organisation for various reasons, such as network segmentation preventing the solution from identifying and reporting from various parts of the enterprise network, endpoint software agents not being fully deployed or functional, and incompatibility across a broad range of disparate technologies. Unfortunately, those assets that are unaccounted for pose the greatest risk. If they are not tracked, they are most likely not receiving the most recent patches and updates, are not replaced during lifecycle refreshments, and malware may be allowed to exploit and maintain its hold of the asset.

Migrating to the cloud provides changes the scenario in terms of asset management. This is because the cloud provider assumes responsibility for managing physical assets that comprise the cloud infrastructure. This can significantly reduce the burden of physical asset management for customers for those workloads that are hosted in the cloud. The customer would still be responsible for maintaining physical asset inventories for the equipment they keep in their environment for instance, datacentres, offices, deployed IoT, mobile workforce and others. This therefore means that the cloud provider has to maintain and avail the inventory list that pertains to the particular SME.

4.5.2 Implementation of the Framework

The framework core represents the life cycle structure of the management process of cyber security, both from a technical and organisational point of view. The core is structured hierarchically into group metrics, metrics and sub metrics. The group metrics are: Identify, Protect, Detect, Respond, Recover and they represent the main topics to deal with in order to strategically secure data in the cloud. Thus, the framework, for each group metrics, metrics and sub metrics, will provide information in terms of specific questions, defines the categories and technologies to be put in place in order to manage the single function.

The priority levels help to support organisations and companies in the preliminary identification of sub metrics to be implemented in order to further reduce their risk levels, while balancing the effort to implement them. The priority levels aid to:

i. Simplify the identification of essential sub metrics to be immediately implemented;
ii. Support the organisations in their risk analysis and management process.

The identification of priority levels assigned to Subcategories have been performed according to two specific criteria:

i. Ability to reduce cyber risk, by working on one or more key factors for the identification, that is, exposure to threats, intended as the set of factors that increase or diminish the threat probability; Occurrence Probability, that is the frequency of the possible event of a threat over the time; impact on business operations and company assets, intended as the amount of damage resulting from the threat occurrence;

ii. Ease of sub metric implementation, considering the technical and organisational maturity usually required to put in place specific countermeasures.

The framework suggests the use of a priority scale of three levels among sub metrics. The combination of these two criteria allows the definition of three different priority levels:

i. High Priority: Actions that enable the slight reduction of one of the three key factors of cyber risk. Such actions are prioritised and must be implemented irrespective of their implementation complexity;
ii. Medium Priority: Actions that enable the reduction of one of the three key factors of cloud security risk, that is generally easily implementable.
iii. Low Priority: Actions that make possible to reduce one of the three key factors of the cloud security risk and that are generally considered as hard to be implemented (Require significant organisational and/or infrastructural changes).

Further, the framework core structure shows validation references that link the single sub metric to a number of known security practices by using internationally recognised security standards like ISO, SP800-53r4, COBIT-5, SANS20 and others.

The classification of the sub levels advises the SME on the rules and procedures that all individuals accessing and using the organisation’s IT assets and resources must follow. The goal of the classifications is to provide details on which aspect of the security needs attention and also who is in charge of doing so.

Table 17 shows details of the framework, its levels, priority, validation reference, which group it applies to, the metric type and the metric classification. The research suggests a score of one (1) point if the answer is yes and score of zero (0) if the answer is no. The total scored subjected to the GQM formula will enable one to work out the indicative of how secure the SME’s cloud data is.

Table 17: Framework Details

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
1	**IDENTIFY RISKS IN CLOUD**				Group Metric	Met_1
1.1	**Asset Administration (1.1):** The information, employees, equipment, structures, and services that allow the SME to achieve business processes are identified and managed consistent with their relative importance to business objectives and the SME's risk strategy.				Metric	$Met_{1.1}$
1.1.1	**ID.AM-1**: Are all physical IT equipment (computers, laptops, BYOD) within the SME inventoried?	HIGH	· COBIT 5 BAI09.01, BAI09.02 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8	SME Administrators need to comply	Sub Metric	$Met_{1.1.1}$
1.1.2	**ID.AM-2:** Are all system and application software within the SME inventoried?	HIGH	· COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8	SME Administrators need to comply	Sub Metric	$Met_{1.1.2}$
1.1.3	**ID.AM-3:** Cloud Providers allow the SME to determine where their content will be stored, how it will be secured in transit or at rest, and managed?	LOW	· COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8	Cloud providers need to provide information	Sub Metric	$Met_{1.1.3}$
1.1.4	**ID.AM-4:** Does the SME ensure that providers of external information system services comply with the SME's information security requirements like applicable laws, directives, policies, regulations, standards, and guidance?	HIGH	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9	SME Administrators need to comply	Sub Metric	$Met_{1.1.4}$
1.1.5	**ID.AM-5:** Does the cloud provider specify what sort of resilience to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)?	MEDIUM	· ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 · COBIT 5 APO03.03, · APO03.04, BAI09.02	Cloud providers need to provide information	Sub Metric	$Met_{1.1.5}$

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
1.2	**Governance (1.2):** The guidelines, policies and methods to manage and monitor the SME's regulatory, legal, risk, environmental, and operational requirements are understood and inform the SME owner(s) of cyber security risk		·		Metric	$Met_{1.2}$
1.2.1	**ID.GV-1:** Has the cloud provider established and communicated a well-informed security policy in relation to the data stored on the cloud?	MEDIUM	· COBIT 5 APO01.03, EDM01.01, EDM01.02 · ISA 62443-2-1:2009 4.3.2.6 · ISO/IEC 27001:2013 A.5.1.1 · NIST SP 800-53 Rev. 4 -1 controls	Cloud providers need to provide information	Sub Metric	$Met_{1.2.1}$
1.2.2	**ID.GV-2:** Are the staff trained regularly on Information security roles & responsibilities including third party providers?	MEDIUM	· COBIT 5 APO13.12 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 · NIST SP 800-53 Rev. 4 PM-1, PS-7	SME Owner / Admin / Users need to be regularly trained	Sub Metric	$Met_{1.2.2}$
1.2.3	**ID.GV-3:** Are legal and regulatory requirements regarding cloud security understood and managed by the SME and explained well by the cloud provider?	HIGH	· COBIT 5 MEA03.01, MEA03.04 · ISO/IEC 27001:2013 A.18.1 · ISA 62443-2-1:2009 4.4.3.7	SME Owner / Admin / Users	Sub Metric	$Met_{1.2.3}$
1.2.4	**ID.GV-4**: Does the cloud provider update the SME on any change pertaining to risk management processes?	LOW	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, · 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · NIST SP 800-53 Rev. 4 PM-9, PM-11	Cloud Provider need to confirm	Sub Metric	$Met_{1.2.4}$

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
1.3	**Risk Assessment (1.3):** The SME understands the cyber security risk to their operations including their operations, image and reputation, assets, and staff.		·	·	Metric	$Met_{1.3}$
1.3.1	**ID.RA-1:** Does the SME update and patch their operating systems and carry out vulnerability scans on their systems regularly?	MEDIUM	· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA- 5, SA-11, SI-2, SI-4, SI-5	SME Administrators need to comply	Sub Metric	$Met_{1.3.1}$
1.3.2	**ID.RA-3:** Does the SME perform a continuous risk assessment process to identify, evaluate and mitigate risks across their company?	LOW	· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16	SME Administrators need to comply	Sub Metric	$Met_{1.3.2}$
1.3.3	**ID.RA-4:** Does the SME identify potential business impacts and likelihoods related to the cloud?	LOW	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14	SME Owner / Admin / Users need to get trained	Sub Metric	$Met_{1.3.3}$
1.3.4	**ID.RA-5**: Threats, vulnerabilities, likelihoods, and impacts in cloud computing are understood well by the SME?	LOW	· COBIT 5 APO12.02 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16	SME Owner / Admin / Users need to get trained	Sub Metric	$Met_{1.3.4}$
1.3.5	**ID.RA-6:** Are cloud Risk responses identified and prioritised?	LOW	· COBIT 5 APO12.05, APO13.02 · NIST SP 800-53 Rev. 4 PM-4, PM-9	SME Owner / Admin / Users need to get trained	Sub Metric	$Met_{1.3.5}$

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
2	**PROTECT DATA IN THE CLOUD**				Group Metric	$M et_{1}$
2.1	**Access Control (2.1):** Access to IT and related equipment, facilities and systems is limited to only authorised personnel and devices and to carry out only authorised actions and transactions.		·	·	Metric	$M et_{2.1}$
2.1.1	**PR.AC-1:** Does the SMEs user credentials for the cloud issued, managed, verified, revoked, and audited for authorised devices, users and processes only?	HIGH	· COBIT 5 DSS05.04, DSS06.03 · ISA 62443-2-1:2009 4.3.3.5.1 · NIST SP 800-53 Rev. 4 AC-2, IA Family	SME Administrator/ Implement authentication technologies ·	Sub Metric	$M et_{2.1.1}$ ·
2.1.2	**PR.AC-2:** Are physical assets protected and access to assets in the SMEs premises managed?	MEDIUM	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 · ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3	SME Owners/ Users. Implement physical controls. ·	Sub Metric	$M et_{2.1.2}$ ·
2.1.3	**PR.AC-3:** Are SMEs establishing and documenting usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed to their systems in accordance with their access control policy?	HIGH	· COBIT 5 APO13.01, DSS01.04, DSS05.03 · ISA 62443-2-1:2009 4.3.3.6.6 · ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1	SME Administrator/ Logging all activities.	Sub Metric	$M et_{2.1.3}$
2.1.4	**PR.AC-4:** Is access to systems by users managed in terms of permissions, implementing the use of least privilege?	HIGH	· CCS CSC 12, 15 · ISA 62443-2-1:2009 4.3.3.7.3 · SA I62443-3-3:2013 SR 2.1 · NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16	SME Administrator to avoid giving access to unauthorised users. ·	Sub Metric	$M et_{2.1.4}$
2.1.5	**PR.AC-5:** Is the SMEs LAN and WAN well protected, including network segregation if applicable?	MEDIUM	· ISA 62443-2-1:2009 4.3.3.4 · ISA 62443-3-3:2013 SR 3.1, SR 3.8 · ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1	SME Administrator t ensure network is secure	Sub Metric	$M et_{2.1.5}$
2.1.6	**PR.AC-7:** Does the cloud provider use appropriate technology like single-factor, multi-factor to ensure that SME users, devices, and other assets are authenticated?	MEDIUM	· COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 · ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4	Cloud Provider	Sub Metric	$M et_{2.1.6}$

Level	Description	Priority	Validation References	Classification	Type	Metric
2.2	**Awareness and Training (2.2):** The SME's users and staff are provided regular security awareness trainings and are sufficiently trained to perform their work whilst ensuring that security is paramount and tasks are performed as outlined in the policies, procedures, and agreements.				Metric	$Met_{2.2}$
2.2.1	**PR.AT-1:** All users are informed and trained on the security aspects pertaining to their cloud usage?	HIGH	· ISO/IEC 27001:2013 A.7.2.2 · NIST SP 800-53 Rev. 4 AT-2, PM-13 · COBIT 5 APO07.03, BAI05.07 · ISA 62443-2-1:2009 4.3.2.4.2	SME Users/ Admin/ Owners be trained well	Sub Metric	$Met_{2.2.1}$
2.2.2	**PR.AT-2:** Do the SME's Privileged users like admins and super users understand their privileges & responsibilities pertaining to the cloud?	HIGH	· CCS CSC 9 · COBIT 5 APO07.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 AT-3, PM-13	SME Users/ Admin/ Owners be trained well	Sub Metric	$Met_{2.2.2}$
2.2.4	**PR.AT-4**: Do the SME's owners and senior personnel understand their privileges & responsibilities pertaining to the cloud?	HIGH	COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13	SME Users/ Admin/ Owners be trained well	Sub Metric	$Met_{2.2.4}$
2.2.5	**PR.AT-5:** Do information security personnel understand their privileges & responsibilities pertaining to the cloud?	MEDIUM	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13	SME Users/Admin	Sub Metric	$Met_{2.2.5}$

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
2.3	**Data Security (2.3):** Information and records (data) are managed consistent with the organisation's risk strategy to protect the confidentiality, integrity, and availability of information.		·	·	Metric	$Met_{2.3}$
2.3.1	**PR.DS-1:** Is the Data protected while at rest in the cloud?	HIGH	· CCS CSC 17 · COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 · ISA 62443-3-3:2013 SR 3.4, SR 4.1 · ISO/IEC 27001:2013 A.8.2.3 · NIST SP 800-53 Rev. 4 SC-28	Cloud Provider/ Use of Encryption	Sub Metric	$Met_{2.3.1}$
2.3.2	**PR.DS-2:** Is the Data protected while in transit (upload/download from the cloud)?	HIGH	· ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 · CCS CSC 17 · ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	Cloud Provider/ Use of TLS	Sub Metric	$Met_{2.3.2}$
2.3.4	**PR.DS-4:** Does the SME have Adequate bandwidth capacity to ensure availability is maintained for data in the cloud?	HIGH	· COBIT 5 APO13.01 · ISA 62443-3-3:2013 SR 7.1, SR 7.2 · ISO/IEC 27001:2013 A.12.3.1	Administrators / Use of secondary link	Sub Metric	$Met_{2.3.4}$
2.3.5	**PR.DS-5:** Does the cloud provider have **a**pproved firewall rule sets and access control lists between network fabrics to restrict the flow of information to specific information system services and counter for multi-tenancy?	MEDIUM	· ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, · A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS- 6, SC-7, SC-8, SC-13, SC-31, SI-4	Cloud Provider	Sub Metric	$Met_{2.3.5}$
2.3.6	**PR.DS-6:** Does the SME or cloud provider employ integrity verification tools to monitor and detect unauthorised changes to organisation's software and information?	LOW	· ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 · ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SI-7	Cloud Provider, use of monitoring tools	Sub Metric	$Met_{2.3.6}$

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
2.4	**Information Protection Processes and Procedures (2.4):** Security policies addressing roles, responsibilities, and scope, processes, and procedures are maintained and used to manage protection of information systems and assets.			·	Metric	$M et_{2.4}$
2.4.1	**PR.IP-1:** Does the SME create and maintain configuration of IT control systems for the cloud as well as internal systems?	HIGH	· COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · CCS CSC 3, 10	Cloud Provider	Sub Metric	$M et_{2.4.1}$
2.4.2	**PR.IP-2:** Does the SME have a System Development Life Cycle to manage cloud and internal systems implemented?	MEDIUM	· COBIT 5 APO13.01 · ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8	SME users	Sub Metric	$M et_{2.4.2}$
2.4.3	**PR.IP-3: Does the SME have** change control processes in place to track changes in the cloud provider's functionality?	MEDIUM	· COBIT 5 BAI06.01, BAI01.06 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-3, CM-4	Cloud Provider to communicate	Sub Metric	$M et_{2.4.3}$
2.4.4	**PR.IP-4:** Does the cloud provider regularly create, test and validate backups of data stored in the cloud?	HIGH	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.9 · ISA 62443-3-3:2013 SR 7.3, SR 7.4 · ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 · NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9	Cloud Provider / Use of offshore backup	Sub Metric	$M et_{2.4.4}$
2.4.6	**PR.IP-6:** Is data in the cloud destroyed according to policy and no copies retained without the SMEs knowledge?	HIGH	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.4.4.4 · NIST SP 800-53 Rev. 4 MP-6	Cloud Provider to ensure ·	Sub Metric	$M et_{2.4.6}$ ·

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
2.4.8	**PR.IP-8:** Does the cloud provider share **e**ffectiveness of protection technologies with the SME?	LOW	· ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4	Cloud Provider	Sub Metric	$Met_{2.4.8}$
2.4.9	**PR.IP-9:** Are Incident Response, Business Continuity and disaster / incident recovery plans) in place and managed well by the cloud provider?	MEDIUM	· COBIT 5 DSS04.03 · ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 · NIST SP 800-53 Rev. 4 CP-2, IR-8	SME Owners	Sub Metric	$Met_{2.4.9}$
2.4.10	**PR.IP-10:** Are the above-mentioned BC and DR plans tested and validated periodically?	LOW	· ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.17.1.3 · NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14	SME Owners / Admin / Cloud Provider ·	Sub Metric	$Met_{2.4.10}$
2.4.12	**PR.IP-12:** Does the SME have a vulnerability management plan in place?	MEDIUM	· ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 · NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2	SME Owners / Admin / Cloud Provider	Sub Metric	$Met_{2.4.12}$
2.4.13	**PR.MA-1:** Does the SME maintain and repair their IT assets in a timely manner and are these repair and maintenance activities approved and logged?	LOW	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.3.3.7 · ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 · NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5	Admins	Sub Metric	$Met_{2.4.13}$
2.4.14	**PR.MA-2: Is** Remote maintenance of the SME's IT assets is approved, logged, and performed in a manner that prevents unauthorised access?	HIGH	· COBIT 5 DSS05.04 · ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 · NIST SP 800-53 Rev. 4 MA-4	Admins	Sub Metric	$Met_{2.4.14}$

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
2.5	**Protective Technology (2.5):** Technical security solutions are managed in a manner that ensures the security and resilience of all IT assets, equipment and systems. Also ensures that the management confers with appropriate policies, procedures, and agreements.				Metric	$Met_{2.5}$
2.5.1	**PR.PT-1:** Are all records pertaining to audits and logs of cloud usage documented and reviewed in accordance with the SME's internal policy?	MEDIUM	· CCS CSC 14 · COBIT 5 APO11.04 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · NIST SP 800-53 Rev. 4 AU Family	Admins to administer logging software or tools	Sub Metric	$Met_{2.5.1}$
2.5.2	**PR.PT-2:** Are any **r**emovable media used in the SME's premises protected and its use restricted according to the SME's policy?	MEDIUM	· COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 2.3 · ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7	Administrator to enforce rules	Sub Metric	$Met_{2.5.2}$
2.5.3	**PR.PT-3:** Is Access to equipment, systems and IT assets controlled in a manner that enforces the least functionality principle?	MEDIUM	· COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, · ISO/IEC 27001:2013 A.9.1.2 · NIST SP 800-53 Rev. 4 AC-3, CM-7 ·	Administrator to enforce rules	Sub Metric	$Met_{2.5.3}$

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
3	**DETECT SECURITY INCIDENTS IN THE CLOUD**		·	·	Group Metric	$M\,et_{3}$
3.1	**Anomalies and Events (3.1):** Unusual or irregular activity is detected in a timely manner and the potential impact of events is understood.		· ·	·	Metric	$M\,et_{3.1}$
3.1.1	**DE.AE-1:** Does the SME manage network operations and data flow for users through the cloud?	**LOW**	· COBIT 5 DSS03.01 · ISA 62443-2-1:2009 4.4.3.3 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4	Administrator	Sub Metric	$M\,et_{3.1.1}$
3.1.2	**DE.AE-2:** Does the SME have measures to detect events and analyse attacks and methods?	**LOW**	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR · 2.12, SR 3.9, SR 6.1, SR 6.2 · ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4	Administrator. Use of IPD/IDS	Sub Metric	$M\,et_{3.1.2}$
3.1.4	**DE.AE-4:** Does the cloud provider give means of determining the impact of events in the cloud?	**MEDIUM**	· COBIT 5 APO12.06 · NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4	Cloud Provider	Sub Metric	$M\,et_{3.1.4}$
3.1.5	**DE.AE-5:** Are incident alert thresholds established by the cloud provider for their cloud services?	**MEDIUM**	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.2.3.10 · NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8	Cloud Provider	Sub Metric	$M\,et_{3.1.5}$

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
3.2	**Security Continuous Monitoring (3.2):** The IT systems and assets are monitored at appropriate intervals to identify any security events and to verify the effectiveness of security controls.			·	Metric	$Met_{3.2}$
3.2.1	**DE.CM-1:** Is the LAN and WAN monitored to detect potential cloud security events?	MEDIUM	· CCS CSC 14, 16 · COBIT 5 DSS05.07 · NIST SP 800-53 Rev. 4 AC-2, AU-12,	Administrator. Use network monitoring tools.	Sub Metric	$Met_{3.2.1}$
3.2.2	**DE.CM-2:** Is the physical IT equipment monitored to detect potential cloud security?	LOW	· ISA 62443-2-1:2009 4.3.3.3.8 · NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20	Cloud Provider / Administrator / Logging	Sub Metric	$Met_{3.2.2}$
3.2.3	**DE.CM-3:** Personnel activity is monitored to detect any breaches and non-repudiation activities?	LOW	· ISA 62443-3-3:2013 SR 6.2 · NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	Administrator / Logging	Sub Metric	$Met_{3.2.3}$
3.2.7	**DE.CM-7:** Is the cloud environment monitored for unauthorised users or connections?	MEDIUM	NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	Administrator / Logging	Sub Metric	$Met_{3.2.7}$
3.2.8	**DE.CM-8:** Are vulnerability scans regularly performed on the cloud environment?	MEDIUM	· COBIT 5 BAI03.10 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-5	Cloud Provider / Administrator /	Sub Metric	$Met_{3.2.8}$

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
3.3	**Detection Processes (3.3):** Threat detection methods and procedures are maintained and tested to ensure timely and adequate awareness of unusual or irregular events.			·	Metric	$M et_{3.3}$
3.3.1	**DE.DP-1:** Does the SME and cloud provider define the roles and responsibilities for all the users to enable accountability for their actions?	LOW	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.4.3.1 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14	Cloud Provider / Administrator /	Sub Metric	$M et_{3.3.1}$
3.3.2	**DE.DP-2:** Do the threat detection measures conform to all relevant requirements?	MEDIUM	· ISA 62443-2-1:2009 4.4.3.2 · ISO/IEC 27001:2013 A.18.1.4 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4	Cloud Provider / Administrator /	Sub Metric	$M et_{3.3.2}$
3.3.3	**DE.DP-3:** Are the above-mentioned measures tested?	LOW	· ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.14.2.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI- 4	Cloud Provider / Administrator /	Sub Metric	$M et_{3.3.3}$
3.3.4	**DE.DP-4:** Are the above-mentioned measures communicated to the SME personnel?	MEDIUM	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.4.5.9 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4	Cloud Provider / Administrator /	Sub Metric	$M et_{3.3.4}$
3.3.5	**DE.DP-5:** Are the above-mentioned measures and processes continuously improved?	LOW	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM- 14	Cloud Provider / Administrator /	Sub Metric	$M et_{3.3.5}$

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
4	**RESPOND TO SECURITY EVENTS IN THE CLOUD**		·	·	Group Metric	$M et_{4}$
4.1	**Response Planning (4.1):** Response procedures and measures are executed and maintained, to ensure timely response to detected cloud security incidents			·	Metric	$M et_{4.1}$
4.1.1	**RS.RP-1:** Is a valid **r**esponse plan executed in case of an event?	LOW	· COBIT 5 BAI01.10 · CCS CSC 18 · ISA 62443-2-1:2009 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8	Cloud Provider / Administrator /	Sub Metric	$M et_{4.1.1}$
4.2	**Communications (4.2):** Response activities are coordinated with the SME, to include external support from law enforcement agencies if applicable.			·	Metric	$M et_{4.2}$
4.2.1	**RS.CO-1:** Do all the staff of the SME know their roles and directive of procedures when a response is required?	LOW	· ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 · NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8	Cloud Provider	Sub Metric	$M et_{4.2.1}$
4.2.2	**RS.CO-2:** Are all events reported in accordance with the established criteria?	LOW	· ISA 62443-2-1:2009 4.3.4.5.5 · ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8	Cloud Provider / Administrator	Sub Metric	$M et_{4.2.2}$
4.2.3	**RS.CO-3:** Is **i**nformation shared between the SME and the cloud provider in accordance with response plans?	LOW	· ISA 62443-2-1:2009 4.3.4.5.2 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4	Cloud Provider / Administrator	Sub Metric	$M et_{4.2.3}$
4.2.4	**RS.CO-4:** Coordination between the SME and the cloud provider occurs in accordance to the response plans?	LOW	· ISA 62443-2-1:2009 4.3.4.5.5 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Cloud Provider / Administrator	Sub Metric	$M et_{4.2.4}$

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
4.3	**Analysis (4.3): Proper a**nalysis is done to confirm sufficient response and recovery undertakings.		·	·	Metric	$Met_{4.3}$
4.3.1	**RS.AN-1:** Are notifications from detection systems investigated appropriately by the cloud providers and administrators?	LOW	· COBIT 5 DSS02.07 · ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	Cloud Provider / Administrator / Logging	Sub Metric	$Met_{4.3.1}$
4.3.2	**RS.AN-2:** Is the impact of any potential incident understood by the SME?	MEDIUM	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4	Users / Administrator / SME Owners	Sub Metric	$Met_{4.3.2}$
4.3.3	**RS.AN-3:** Are forensics for any potential security incident performed?	LOW	· ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR · 2.12, SR 3.9, SR 6.1 · ISO/IEC 27001:2013 A.16.1.7 · NIST SP 800-53 Rev. 4 AU-7, IR-4	Cloud Provider	Sub Metric	$Met_{4.3.3}$
4.3.4	**RS.AN-4:** Are incidents categorised based on the response plans?	LOW	· ISA 62443-2-1:2009 4.3.4.5.6 · ISO/IEC 27001:2013 A.16.1.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8	Cloud Provider	Sub Metric	$Met_{4.3.4}$

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
4.4	**Mitigation (4.4): Strategic a**ctivities are performed to prevent further escalation of a security incident, and measures to mitigate and eliminate the threat.		·	·	Metric	$Met_{4.4}$
4.4.1	**RS.MI-1:** Incidents in the cloud are contained when they occur as per previous reports?	HIGH	· ISA 62443-2-1:2009 4.3.4.5.6 · ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4	Cloud Provider	Sub Metric	$Met_{4.4.1}$
4.4.2	**RS.MI-2:** Incidents in the cloud are mitigated when they occur as per previous reports?	HIGH	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 · ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4	Cloud Provider	Sub Metric	$Met_{4.4.2}$
4.4.3	**RS.MI-3:** Are any new vulnerabilities mitigated or documented as accepted risks?	HIGH	· ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5	Cloud Provider	Sub Metric	$Met_{4.4.3}$
4.5	**Improvements (4.5):** SME's response activities are improved by incorporating lessons learned from current and previous detection/response activities			·	Metric	$Met_{4.5}$
4.5.1	**RS.IM-1:** Are response plans updates to include lessons learned?	LOW	· COBIT 5 BAI01.13 · ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Cloud Provider / Admin	Sub Metric	$Met_{4.5.1}$
4.5.2	**RS.IM-2:** Are response strategies updated accordingly?	LOW	· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Cloud Provider / Admin	Sub Metric	$Met_{4.5.2}$

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
	RECOVER FROM BREACHES IN THE CLOUD			·	Group Metric	$M et_{5}$
5.1	**Recovery Planning (5.1):** Recovery procedures and techniques are performed and continued to make sure apt restoration of IT systems or assets that may be affected by the security events.			·	Metric	$M et_{5.1}$
5.1.1	**RC.RP-1: Is the r**ecovery plan effected in case of an event?	MEDIUM	· CCS CSC 8 · COBIT 5 DSS02.05, DSS03.04 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8	Cloud Provider	Sub Metric	$M et_{5.1.1}$
5.2	**Improvements (5.2):** Recovery planning and techniques are continuously upgraded by including lessons learned.		·	·	Metric	$M et_{5.2}$
5.2.1	**RC.IM-1:** Do all **r**ecovery documents include lessons learned?	LOW	· COBIT 5 BAI05.07 · ISA 62443-2-1 4.4.3.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Cloud Provider / Admin	Sub Metric	$M et_{5.2.1}$
5.2.2	**RC.IM-2: Are all the r**ecovery strategies updated?	LOW	· COBIT 5 BAI07.08 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Cloud Provider / Admin	Sub Metric	$M et_{5.2.2}$
5.3	**Communications (5.3):** Restoration activities are coordinated with the SMEs			·	Metric	$M et_{5.3}$
5.3.3	**RC.CO-3:** Restoration accomplishments are communicated to SME teams.	MEDIUM	· NIST SP 800-53 Rev. 4 CP-2, IR-4	Cloud Provider	Sub Metric	$M et_{5.3.3}$

4.5.3 Testing the Framework Functionality

The Security Index (IndSec) is defined as the highest value in a set of security items:

IndSec = max ($M\,et_1, M\,et_2, M\,et_3, M\,et_4, M\,et_5$)

Example 1, max($M\,et_1, M\,et_2, M\,et_3, M\,et_4, M\,et_5$) = max(1,1,1,1,1) = 1.

Therefore, IndSec = 1, meaning the cloud environment is secure.

Example 2, max($M\,et_1, M\,et_2, M\,et_3, M\,et_4, M\,et_5$) = max(1,0,1,0,0) = 0.

Therefore, IndSec = 0, meaning the cloud environment is not secure.

The use of the function max at each level of hierarchy causes the largest measured metric value to be passed on to the level. Immediately above, i.e. the highest measured value will be the only significant one.

The value of a metric group ($M\,et_x$) is defined as the highest value from a set of metrics:

Met_x = max ($Met_{x.1}, Met_{x.2}, ..., Met_{x.n}$). For instance, Met_1 = max ($Met_{1.1}, Met_{1.2}, Met_{1.3}$).

An example for a best-case scenario is as below:

Met_1= max ($Met_{1.1}$, $Met_{1.2}$, $Met_{1.3}$).

Met_1= max ($1,1,1$).

Met_1= 1

Met_2= max ($Met_{2.1}, Met_{2.2}, Met_{2.3}, Met_{2.4}, Met_{2.5}$).

Met_2= max ($1,1,1,1,1$).

Met_2= 1

Met_3= max ($Met_{3.1}, Met_{3.2}, Met_{3.3}$).

Met_3= max ($1,1,1$).

Met_3= 1

Met_4= max ($Met_{4.1}$, $Met_{4.2}$, $Met_{4.3}$, $Met_{4.4}$, $Met_{4.5}$).

Met_4= max ($1,1,1,1,1$).

Met_4 = 1

Met_5= max ($Met_{5.1}, Met_{5.2}, Met_{5.3}$).

Met_5= max ($1,1,1$).

$Met_{5=}$ 1

On the flip side, a non-secure scenario result is represented below:

Met_1= max ($Met_{1.1}$, $Met_{1.2}$, $Met_{1.3}$).

Met_1= max ($1,0,0$).

Met_1= 0

Met_2= max ($Met_{2.1}$,$Met_{2.2}$,$Met_{2.3}$,$Met_{2.4}$,$Met_{2.5}$).

Met_2= max ($1,1,0,0,0$).

Met_2= 0

Met_3= max ($Met_{3.1}$,$Met_{3.2}$,$Met_{3.3}$).

Met_3= max ($0,0,0$).

Met_3= 0

Met_4= max ($Met_{4.1}$, $Met_{4.2}$, $Met_{4.3,}$ $Met_{4.4}$, $Met_{4.5}$).

Met_4= max ($0,1,0,0,0$).

Met_4 = 0

Met_5= max ($Met_{5.1}$,$Met_{5.2}$,$Met_{5.3}$).

Met_5= max ($1,0,0$).

$Met_{5=}$ 0

The value of a metric ($Met_{x.y}$) is defined as the highest value from a set of sub-metrics: $Met_{x.y}$ = max ($Met_{x.y.1}$, $Met_{x.y.2}$, ..., $Met_{x.y.n}$). For instance, $Met_{1.1}$ = max ($Met_{1.1.1}$, $Met_{1.1.2}$, $Met_{1.1.3,}$ $Met_{1.1.4}$, $Met_{1.1.5}$).

An example for a best-case scenario is as below:

$Met_{1.1}$= max ($Met_{1.1.1}$, $Met_{1.1.2}$, $Met_{1.1.3}$, $Met_{1.1.4}$, $Met_{1.1.5}$).

$Met_{1.1}$= max ($1,1,1,1,1$).

$Met_{1.1}$= 1

$Met_{1.2}$= max ($Met_{1.2.1}$, $Met_{1.2.2}$, $Met_{1.2.3,}$ $Met_{1.2.4}$).

$Met_{1.2}$= max ($1,1,1,1)$.

$Met_{1.2}$= 1

$Met_{1.3}$= max ($Met_{1.3.1}$, $Met_{1.3.2}$, $Met_{1.3.3}$, $Met_{1.3.4}$, $Met_{1.3.5}$).

$Met_{1.3}$= max ($1,1,1,1,1$).

$Met_{1.3}$= 1

On the flip side, a non-secure scenario result is represented below:

$Met_{1.1}$= max ($Met_{1.1.1}$, $Met_{1.1.2}$, $Met_{1.1.3}$, $Met_{1.1.4}$, $Met_{1.1.5}$).

$Met_{1.1}$= max $(1,0,0,0,1)$.

$Met_{1.1}$= 0

$Met_{1.2}$= max $(Met_{1.2.1}, Met_{1.2.2}, Met_{1.2.3,} Met_{1.2.4})$.

$Met_{1.2}$= max $(0,0,0,1)$.

$Met_{1.2}$= 0

$Met_{1.3}$= max $(Met_{1.3.1}, Met_{1.3.2}, Met_{1.3.3}, Met_{1.3.4}, Met_{1.3.5})$.

$Met_{1.3}$= max $(0,0,0,0,0)$.

$Met_{1.3}$= 0

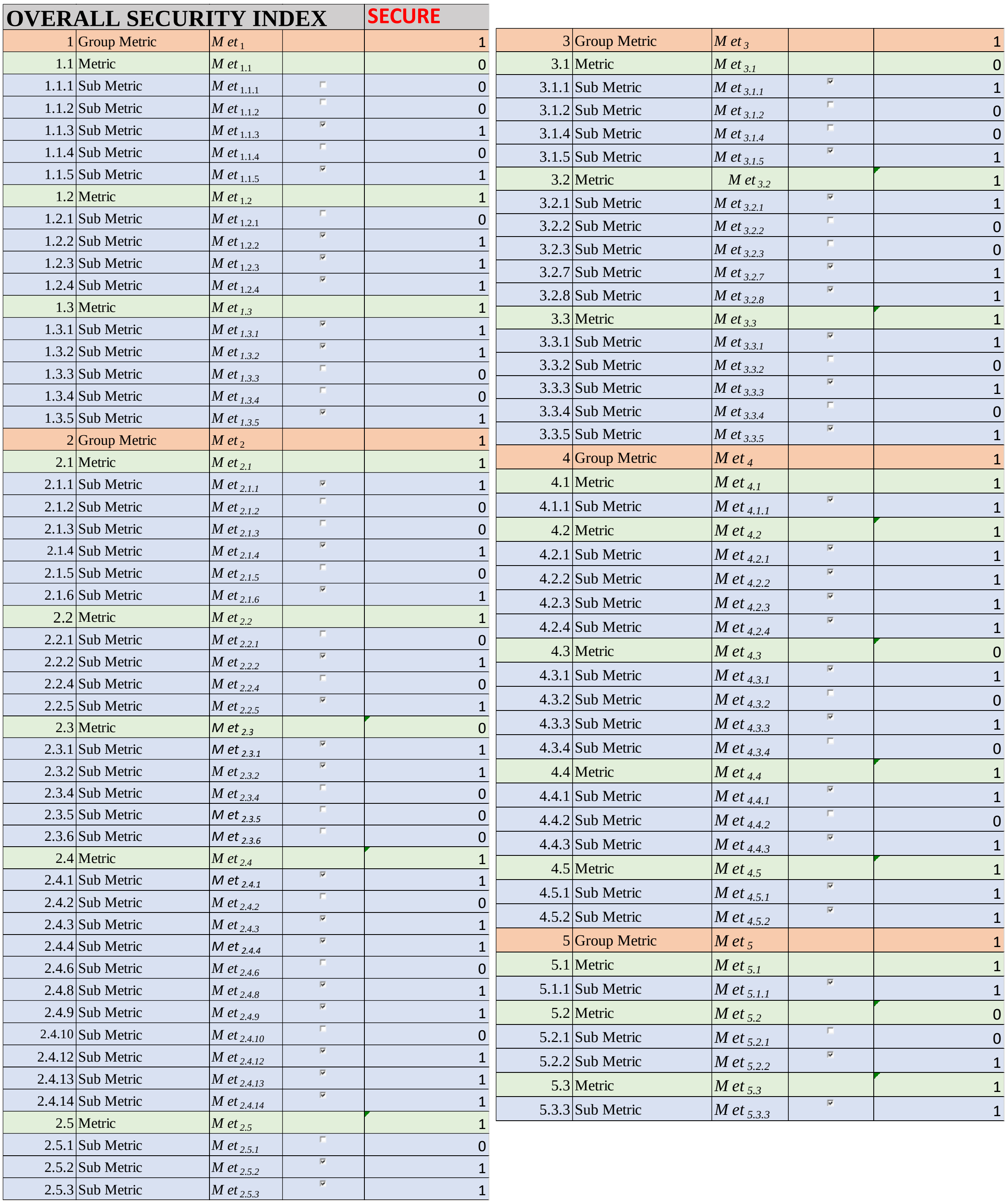
The sub-metric $M\ et_{x,y,n}$ either yields a 1(based on a yes) or a 0(based on a no). For example, $M\ et_{2.3.2}$ - *Is the Data protected while in transit (upload/download from the cloud)? Yes.*

Then $M\ et_{2.3.2}=1$

$M\ et_{2.3.2}$ - *Is the Data protected while in transit (upload/download from the cloud)? No.*

Then, $M\ et_{2.3.2}=0$

If the above metrics are used to compute the security index of an SME X, we will get an either secure or not secure result. A typical scenario is illustrated in Figure 18.



OVERALL SECURITY INDEX				SECURE
1	Group Metric	$M\,et_{1}$		1
1.1	Metric	$M\,et_{1.1}$		0
1.1.1	Sub Metric	$M\,et_{1.1.1}$	☐	0
1.1.2	Sub Metric	$M\,et_{1.1.2}$	☐	0
1.1.3	Sub Metric	$M\,et_{1.1.3}$	☑	1
1.1.4	Sub Metric	$M\,et_{1.1.4}$	☐	0
1.1.5	Sub Metric	$M\,et_{1.1.5}$	☑	1
1.2	Metric	$M\,et_{1.2}$		1
1.2.1	Sub Metric	$M\,et_{1.2.1}$	☐	0
1.2.2	Sub Metric	$M\,et_{1.2.2}$	☑	1
1.2.3	Sub Metric	$M\,et_{1.2.3}$	☑	1
1.2.4	Sub Metric	$M\,et_{1.2.4}$	☑	1
1.3	Metric	$M\,et_{1.3}$		1
1.3.1	Sub Metric	$M\,et_{1.3.1}$	☑	1
1.3.2	Sub Metric	$M\,et_{1.3.2}$	☑	1
1.3.3	Sub Metric	$M\,et_{1.3.3}$	☐	0
1.3.4	Sub Metric	$M\,et_{1.3.4}$	☐	0
1.3.5	Sub Metric	$M\,et_{1.3.5}$	☑	1
2	Group Metric	$M\,et_{2}$		1
2.1	Metric	$M\,et_{2.1}$		1
2.1.1	Sub Metric	$M\,et_{2.1.1}$	☑	1
2.1.2	Sub Metric	$M\,et_{2.1.2}$	☐	0
2.1.3	Sub Metric	$M\,et_{2.1.3}$	☐	0
2.1.4	Sub Metric	$M\,et_{2.1.4}$	☑	1
2.1.5	Sub Metric	$M\,et_{2.1.5}$	☐	0
2.1.6	Sub Metric	$M\,et_{2.1.6}$	☑	1
2.2	Metric	$M\,et_{2.2}$		1
2.2.1	Sub Metric	$M\,et_{2.2.1}$	☐	0
2.2.2	Sub Metric	$M\,et_{2.2.2}$	☑	1
2.2.4	Sub Metric	$M\,et_{2.2.4}$	☐	0
2.2.5	Sub Metric	$M\,et_{2.2.5}$	☑	1
2.3	Metric	$M\,et_{2.3}$		0
2.3.1	Sub Metric	$M\,et_{2.3.1}$	☑	1
2.3.2	Sub Metric	$M\,et_{2.3.2}$	☑	1
2.3.4	Sub Metric	$M\,et_{2.3.4}$	☐	0
2.3.5	Sub Metric	$M\,et_{2.3.5}$	☐	0
2.3.6	Sub Metric	$M\,et_{2.3.6}$	☐	0
2.4	Metric	$M\,et_{2.4}$		1
2.4.1	Sub Metric	$M\,et_{2.4.1}$	☑	1
2.4.2	Sub Metric	$M\,et_{2.4.2}$	☐	0
2.4.3	Sub Metric	$M\,et_{2.4.3}$	☑	1
2.4.4	Sub Metric	$M\,et_{2.4.4}$	☑	1
2.4.6	Sub Metric	$M\,et_{2.4.6}$	☐	0
2.4.8	Sub Metric	$M\,et_{2.4.8}$	☑	1
2.4.9	Sub Metric	$M\,et_{2.4.9}$	☑	1
2.4.10	Sub Metric	$M\,et_{2.4.10}$	☐	0
2.4.12	Sub Metric	$M\,et_{2.4.12}$	☑	1
2.4.13	Sub Metric	$M\,et_{2.4.13}$	☑	1
2.4.14	Sub Metric	$M\,et_{2.4.14}$	☑	1
2.5	Metric	$M\,et_{2.5}$		1
2.5.1	Sub Metric	$M\,et_{2.5.1}$	☐	0
2.5.2	Sub Metric	$M\,et_{2.5.2}$	☑	1
2.5.3	Sub Metric	$M\,et_{2.5.3}$	☑	1

3	Group Metric	$M\,et_{3}$		1
3.1	Metric	$M\,et_{3.1}$		0
3.1.1	Sub Metric	$M\,et_{3.1.1}$	☑	1
3.1.2	Sub Metric	$M\,et_{3.1.2}$	☐	0
3.1.4	Sub Metric	$M\,et_{3.1.4}$	☐	0
3.1.5	Sub Metric	$M\,et_{3.1.5}$	☑	1
3.2	Metric	$M\,et_{3.2}$		1
3.2.1	Sub Metric	$M\,et_{3.2.1}$	☑	1
3.2.2	Sub Metric	$M\,et_{3.2.2}$	☐	0
3.2.3	Sub Metric	$M\,et_{3.2.3}$	☐	0
3.2.7	Sub Metric	$M\,et_{3.2.7}$	☑	1
3.2.8	Sub Metric	$M\,et_{3.2.8}$	☑	1
3.3	Metric	$M\,et_{3.3}$		1
3.3.1	Sub Metric	$M\,et_{3.3.1}$	☑	1
3.3.2	Sub Metric	$M\,et_{3.3.2}$	☐	0
3.3.3	Sub Metric	$M\,et_{3.3.3}$	☑	1
3.3.4	Sub Metric	$M\,et_{3.3.4}$	☐	0
3.3.5	Sub Metric	$M\,et_{3.3.5}$	☑	1
4	Group Metric	$M\,et_{4}$		1
4.1	Metric	$M\,et_{4.1}$		1
4.1.1	Sub Metric	$M\,et_{4.1.1}$	☑	1
4.2	Metric	$M\,et_{4.2}$		1
4.2.1	Sub Metric	$M\,et_{4.2.1}$	☑	1
4.2.2	Sub Metric	$M\,et_{4.2.2}$	☑	1
4.2.3	Sub Metric	$M\,et_{4.2.3}$	☑	1
4.2.4	Sub Metric	$M\,et_{4.2.4}$	☑	1
4.3	Metric	$M\,et_{4.3}$		0
4.3.1	Sub Metric	$M\,et_{4.3.1}$	☑	1
4.3.2	Sub Metric	$M\,et_{4.3.2}$	☐	0
4.3.3	Sub Metric	$M\,et_{4.3.3}$	☑	1
4.3.4	Sub Metric	$M\,et_{4.3.4}$	☐	0
4.4	Metric	$M\,et_{4.4}$		1
4.4.1	Sub Metric	$M\,et_{4.4.1}$	☑	1
4.4.2	Sub Metric	$M\,et_{4.4.2}$	☐	0
4.4.3	Sub Metric	$M\,et_{4.4.3}$	☑	1
4.5	Metric	$M\,et_{4.5}$		1
4.5.1	Sub Metric	$M\,et_{4.5.1}$	☑	1
4.5.2	Sub Metric	$M\,et_{4.5.2}$	☑	1
5	Group Metric	$M\,et_{5}$		1
5.1	Metric	$M\,et_{5.1}$		1
5.1.1	Sub Metric	$M\,et_{5.1.1}$	☑	1
5.2	Metric	$M\,et_{5.2}$		0
5.2.1	Sub Metric	$M\,et_{5.2.1}$	☐	0
5.2.2	Sub Metric	$M\,et_{5.2.2}$	☑	1
5.3	Metric	$M\,et_{5.3}$		1
5.3.3	Sub Metric	$M\,et_{5.3.3}$	☑	1

Figure 18: Framework Results
Source: *Framework*

4.6 Chapter Summary

Chapter four presented the findings and interpretation of the study. The data was collected using questionnaires as well as experimental analysis using open source software OwnCloud. Experimental analysis was then carried out with stored data to identify potential security risks in the cloud. The Statistical Package for Social Sciences (SPSS) version 20 was used to analyse the data collected by questionnaires.

The author developed an eight-stage cloud security framework divided in two sections. The first five stages are Identify, Protect, Detect, Respond and Recover. The second section includes Metric Hierarchy, Index of Security and finally Implementation of a Secure Cloud.
The framework was effectively verified using standards and tested for functionality.

CHAPTER FIVE
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

Chapter one provided the background information to the study, an overview of cloud computing, the different paradigms and importance of cloud computing for SMEs in Kenya. The threats and vulnerabilities of the cloud were highlighted forming basis of the research. It was on the basis of this background that the statement of the problem was identified both in specific and general forms, objectives and significance of the study were outlined. Research questions, justification of the study and the scope of the research were also highlighted.

Chapter two highlighted the literature review whereby the properties of cloud computing as well as the benefits were discussed in details. Thereafter the challenges of cloud computing were highlighted and the areas of concern in cloud computing were outlined. Confidentiality, Integrity and Availability issues in the cloud were also highlighted and cloud computing trends in Africa and Kenya were discussed. Related frameworks and studies relevant to this research were reviewed and the framework building blocks were discussed. Finally, the conceptual framework described the problem and how various variables operate in influencing the problem.

Chapter three described the methodology used in the research. Mixed research methodology comprising of experimental and descriptive research designs were used in this study and finally goal question metrics methodology was used to formulate the cloud security indices. In experimental research design, the researcher used OwnCloud in demonstrating how threats may affect the data in relation to storage and transfer in the cloud and the researcher further used questionnaires to highlight the security challenges faced by SMEs.

Chapter four presented the findings and interpretation of the study. The data was collected using questionnaires as well as experimental analysis using open source software OwnCloud. Experimental analysis was then carried out with stored data to identify potential security risks in the cloud. The Statistical Package for Social Sciences (SPSS) version 20 was used to analyse the data collected by questionnaires. Further to this, the framework was developed using GQM methodology, verified using standards and tested for functionality.

This chapter provided details on how to use the framework effectively and also provided a test case scenario for the framework. Lastly, the summary, conclusion and recommendations for the entire research were done. To close the chapter, suggestions for further research were also outlined.

5.2 Using the Framework

The implementation of the Framework by a SME should be performed in five steps, as showed in Figure 19.

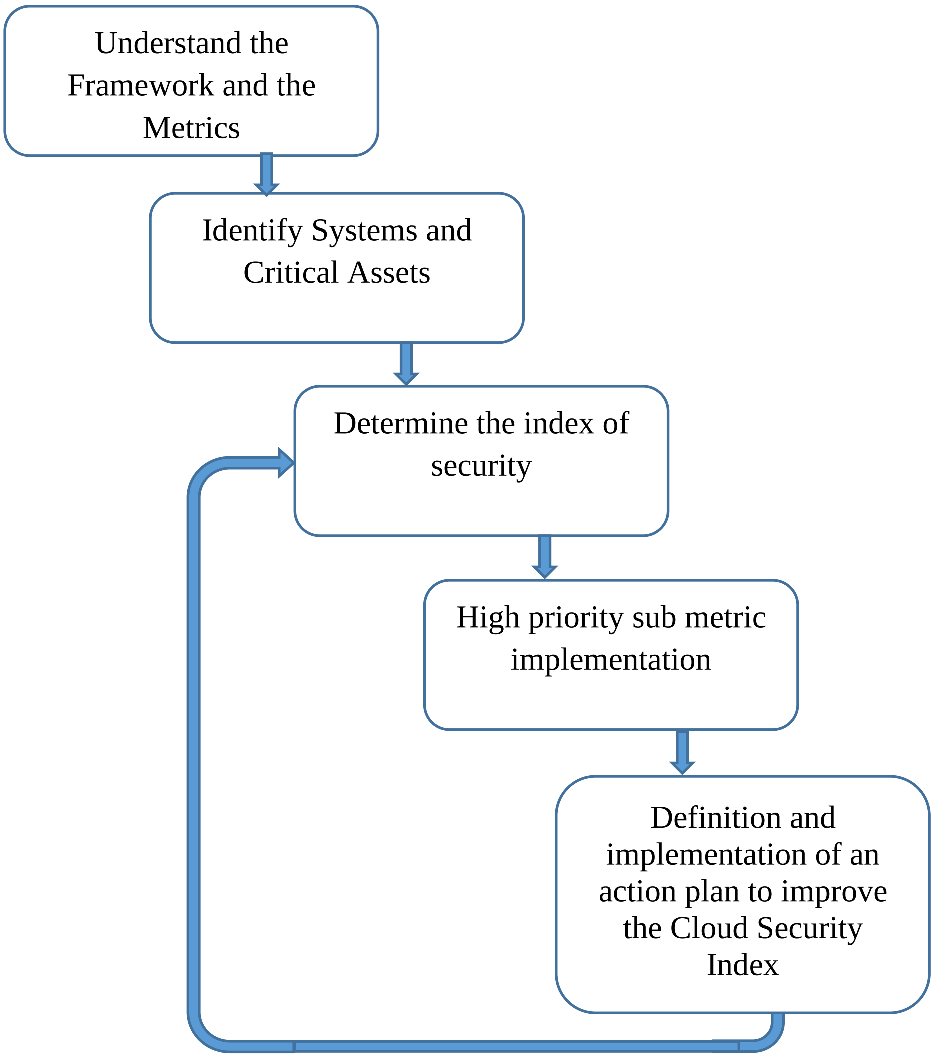

Understand the Framework and the Metrics
Identify Systems and Critical Assets
Determine the index of security
High priority sub metric implementation
Definition and implementation of an action plan to improve the Cloud Security Index

Figure 19: Using the Framework for Improving Security in Cloud Computing
Source: *Author* (2019)

The steps are explained as follows:

i. **Understand the Framework and the Metrics**. The SME has to understand the framework and its sub components for its business objectives and its security pertaining to the cloud. This activity can be performed also starting from a publicly available contextualisation and adjusting it to the specific business context of the SME. The questions representing the contextualisation are structured in a logical manner with a yes or no as an answer.

ii. **Identify Systems and Critical Assets**. The identification of ICT systems and information considered crucial or anyway critical by the SME to ensure its operations. This step is important especially for the following stages, as it makes possible to properly evaluate the impacts during risk analysis and it makes easier to understand the actual needed protection. It should be noted that within SMEs it is important to also identify the ones who are responsible for the implementation of the Framework steps for each sub metric.

iii. **Determine the index of security**. Once the sub metric questions have been answered, the answers are subjected to the GQM metrics to be able to determine the index of security which can be either *secure* or *not secure*.

iv. **High priority sub metric implementation**. The SME should start to use the Framework by implementing the high priority sub metrics. This is a critical step in the Framework implementation and it makes possible to reach a degree of preparedness and awareness of the cloud security risk. The target (turning all sub metrics into positive responses) represents the reference to compare the current profile, thus establishing the existing gaps within the cyber security management.

v. **Definition and implementation of an action plan to improve the Cloud Security Index**. The last step of the process of Framework endorsement consists in defining the set of activities needed to reach a secure security index. This means to establish a specific plan to implement the Framework security practices, according to a schedule, that varies upon the actual identified risks and specific conditions of the SME business.

Clearly it is preferable to have a continuous evolution of the Framework implementation, even after having reached the target profile, in line with the cyclic risk assessment staged and following actions of steady improvement.

5.3 Summary

Cloud computing present different risks to an SME as compared to those that traditional IT solutions can solve. As the use of cloud computing are scaled up to larger and larger systems, it is becoming extremely important to find effective frameworks and models for cloud security before deploying to a larger scale in any organisation. The research was focused on improving security in cloud computing for SMEs by the use of a cloud security framework.

The objectives of the study were met. The fundamental cloud security challenges experienced by selected SMEs in Kenya were determined. On fundamental challenges, the findings of the research established that cloud computing face substantial challenges in the implementation of SaaS delivery model. Some of the challenges found include: Data/information stored on the cloud issues on downtime in the internet; cloud administrators are exposed to high risk, if they turn rouge and try to access data stored on clouds; lack of certainty in trailing actions of the users, there is no definite way of telling that the data has been deleted to its entirety; there is no control over the hardware, technology and backed up details of the cloud platform; multi-tenancy issues- there is risk that hackers can manipulate weakness in data security model to get an illegitimate access to data or application; and lack of liability in case of security incidences as a result of cloud computing and subsequent misuse of privileges to gain access or support third parties in accessing data/information they are not meant to access, which further interferes with confidentiality and integrity of information within the cloud service.

On sufficiency of security measures, the findings of the study established that cloud computing service providers make significant effort to put in place stringent security measures. Some of the things they have put in place include; user access control rules, security policies and enforcement, maintaining proper security monitoring logs and random audit, among others. However, cloud providers do not have sufficient and credible policies and practices on data retention, deletion and security; they do not allow clients to carry out audits and multi-tenant hosted by 3rd party usually exposes functionality that could result security issues and they lack relevant recovery procedures for data. Hence, there is considerable concern on integrity of services and privacy of data confidentiality and there is lack of liability on providers in case of security incidents.

A framework was thereafter developed to address the challenges determined in the selected SMEs in Kenya. The framework will play a pivotal role in improving of security in cloud computing solutions in SMEs. The developed framework components were informed by different features from other documented cloud security models and standards such as ENISA, ISO27001 and ISO27002, COSO, ITIL and ISACA. The author proposed an eight-stage cloud security framework divided in two sections. The first five stages being Identify, Protect, Detect, Respond and Recover. The second section includes Metric Hierarchy, Index of Security and finally Implementation of a Secure Cloud. The framework includes measurements of both organisational 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 SMEs in the cloud.

The framework also developed an effective measure of security in the cloud by using cloud security metrics. The research used GQM methodology to come up with group metrics, metrics and sub metrics. Each sub metric was translated into a security question that helps the SME determine the index of security.

Each of the sub metric of the developed framework was validated using international security standards like COBIT, ITIL, ISO 27001, and NIST to ensure that they conform to the security benchmarks set in the security world.

5.4 Conclusion

Cloud computing offers many opportunities to SMEs, but risks and challenges as well. For an SME to succeed, they must critically examine available data, create policies especially security policies, follow existing standards and develop adequate procedures of ensuring adherence. This research offers a means for SMEs to implement cloud solutions in a more secure way, by an approach that is oriented on most of the stages that an organisation must go through to achieve a relatively secure cloud environment.

Standardised frameworks such as FISCCS make a significant impact and create healthy competition among Cloud providers to satisfy their Service Level Agreement (SLA) and improve their Quality of Services (QoS) as well as give SMEs an opportunity to store data in the cloud in a more secure manner as well as increase their trust in the cloud and the cloud provider. 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.

The framework further gives a guiding strategy and procedure to SMEs who wish to develop a cloud security policy by telling them what to secure at which stage and how to do it. It further also gives IT technicians a better idea on how processes flow in the cloud and thereby allowing them to solve security related problems in an informed manner.

5.5 Recommendations

The researcher recommends the following for the SMEs:

The SME in its entirety needs to recognise and understand the value of the cloud-based technology and data as well as the risks. There must be constant vigilance and continuous monitoring of risk to these information assets, including ensuring compliance with appropriate laws, regulations, policies and frameworks.

All users of the cloud should have knowledge of cloud computing and its risks, understand their responsibilities and be accountable for their use of the cloud. From the study findings, the following recommendations were made:

The cloud computing service providers should work closely with their clients on security and confidentiality of their services/data especially on policies and practices on data retention and deletion, and develop relevant recovery procedures for data.

The cloud service providers should find a way of allowing clients to carry out audits on multi-tenant hosted by 3rd party in a manner that it does not expose functionality that cause security concerns.

Both local and national governments should step up in their bid to provide reliable internet to reduce issues of downtime occasioned with internet outage.

The managers of SMEs should employ qualified IT staff with high integrity to reduce chance of internal and external hacking.

5.6 Suggestions for Further Research

The following areas are suggested for further research:

i. The role of the government in promoting development of cloud services in Kenya.

ii. The influence of implementation of SaaS delivery model on growth and profitability of SMEs in Kenya.

iii. Factors impeding the adoption of virtualisation and cloud computing technologies in the Kenyan SMEs industry

REFERENCES

Adeyeye, A. (2016, December). Challenges to SME growth in Kenya. In *Africa Business Insight: Academic Conferences*.

Akhusama, P. M., & Moturi, C. (2016). Cloud computing adoption in insurance companies in Kenya. *American Journal of Information Systems, 4*(1), 11-16.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300). Springer, Berlin, Heidelberg.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., ... & Zaharia, M. (2010). A view of Cloud Computing. *Communications of the ACM. 53*, 5058.

Becker, J. D., & Bailey, E. (2014). IT controls and governance in cloud computing. In *Proceedings of the Twentieth Americas Conference on Information Systems (AMCIS '14)* (pp. 1-8).

Băsescu , C., Carpen-Amarie, A., Leordeanu, C., Costan, A., & Antoniu, G. (2011, March). Managing data access on clouds: A generic framework for enforcing security policies. In *2011 IEEE International Conference on Advanced Information Networking and Applications* (pp. 459-466). IEEE.

Bass, T., & Robichaux, R. (2001). Defence-in-depth revisited: Qualitative risk analysis methodology for complex network-centric operations. In *2001 MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force (Cat. No. 01CH37277)* (Vol. 1, pp. 64-70). IEEE.

Behl, A. (2011, December). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In *2011 World Congress on Information and Communication Technologies* (pp. 217-222). IEEE.

Bhardwaj, S., Jain, L., & Jain, S. (2010). An approach for investigating perspective of cloud software-as-a-service (SaaS). *International Journal of Computer Applications*, *10*(2), 40-43.

Bowen, M., Morara, M., & Mureithi, M. (2009). Management of business challenges among small and micro enterprises in Nairobi-Kenya. *KCA Journal of Business Management*, *2*(1), 16-31.

Buyya, R., Broberg, J., & Goscinski, A. M. (Eds.). (2010). *Cloud computing: Principles and paradigms* (Vol. 87). John Wiley & Sons.

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

Caldiera, V. R. B. G., & Rombach, H. D. (1994). The goal question metric approach. *Encyclopaedia of Software Engineering,* 528-532.

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. *Congressional Research Service Documents, CRS RL32331 (Washington, DC),* 2.

Centre of Internet Security (2016). Retrieved July 4, 2018, from *https://www.cisecurity.org/*

Central Bank of Kenya. (2017). *Annual Report and Financial Statements*.

Chuang, I. H., Li, S. H., Huang, K. C., & Kuo, Y. H. (2011, February). An effective privacy protection scheme for cloud computing. In *13th International Conference on Advanced Communication Technology (ICACT2011)* (pp. 260-265). IEEE.

Centre for the Protection of National Infrastructure (CPNI). (2010). *Information Security Briefing*.

Creswell, J. W. (2014). *A concise introduction to mixed methods research*. Sage Publications.

Culp, C. L. (2002). *The risk management process: Business strategy and tactics* (Vol. 103). John Wiley & Sons.

Daniel, W. K. (2014, April). Challenges on privacy and reliability in cloud computing security. In *2014 International Conference on Information Science, Electronics and Electrical Engineering* (Vol. 2, pp. 1181-1187). IEEE.

Dash, S. B., Saini, H., Panda, T. C., & Mishra, A. (2014). A theoretical aspect of cloud computing service models and its security issues: A Paradigm. *Journal of Engineering Research and Applications,* 4(6), 248-254.

Delettre, C., Boudaoud, K., & Riveill, M. (2011, June). Cloud computing, security and data concealment. In *2011 IEEE Symposium on Computers and Communications (ISCC)* (pp. 424-431). IEEE.

Denning, D. E. (2003). Information technology and security. In Brown, M. (Ed.). *Grave New World: Global Dangers in the 21st Century*. Georgetown University Press.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Commun. ACM, 43*(7), 125-128.

Donald, K. K., & Delno, L. A. T. (2006). *Proposal and Thesis writing: An introduction*. Nairobi Kenya: Pauline Publications Africa.

Dooley, B. (2010). Architectural requirements of the hybrid cloud. *Information Management Online*, *10*.

Ebrahim, Z., & Irani, Z. (2005). E-government adoption: Architecture and barriers. *Business Process Management Journal*, *11*(5), 589-611.

Ellefsen, I. D., & von Solms, S. H. (2012). *Framework for cybersecurity structure in developing countries*. University of Johannesburg.

Erl, T., Puttini, R., & Mahmood, Z. (2013). *Cloud computing: Concepts, technology & architecture*. Pearson Education.

Feng, J., Chen, Y., Ku, W. S., & Liu, P. (2010, September). Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data storage platforms. In *2010 39th International Conference on Parallel Processing Workshops* (pp. 251-258). IEEE.

Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., ... & Stoica, I. (2009). Above the clouds: A Berkeley view of cloud computing. *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS*, *28*(13), 2009.

Frankel, J. R., & Wallen, N. E. (2009). *Single-subject research: How to design and evaluate research in education*. (7th Ed.). New York, NY: McGraw-Hill.

Gallivan, M. J. (2001). Organisational adoption and assimilation of complex technological innovations: Development and application of a new framework. *ACM SIGMIS Database: The Database for Advances in Information Systems*, *32*(3), 51-85.

Gartner. (2018) Retrieved May 14, 2018 from *https://www.gartner.com/it-glossary*

George, E., Louw, D., & Badenhorst, G. (2008). Job satisfaction among urban secondary school teachers in Namibia. *South African Journal of Education*, *28*(2), 135-154.

Granneman, J. (2017). IT security frameworks and standards: Choosing the right one. *TechTarget*.

Harries, D., & Yellowlees, P. M. (2013). Cyberterrorism: Is the US healthcare system safe? *Telemedicine and e-Health*, *19*(1), 61-66.

Hayden, L. (2010). *IT security metrics: A practical framework for measuring security & protecting data*. McGraw-Hill Education Group.

Herrmann, D. S. (2001). *A practical guide to security engineering and information assurance*. Auerbach Publications.

Herrmann, D. S. (2007). *Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and ROI*. Auerbach Publications.

Hooks, C.C., & Duncombe B. (2001). *Handbook for entrepreneurs in developing countries*. University of Manchester, UK.

Hurwitz, J. S., Bloor, R., Kaufman, M., & Halper, F. (2010). *Cloud computing for dummies*. John Wiley & Sons.

International Telecommunications Union (ITU), (2011). *International Multilateral Partnership Against Cyber Threats (IMPACT)*. ITU.

International Telecommunications Union (ITU). 2012

Ionescu, B. S., & Tudoran, L. E. (2013). Financial information security in the cloud. *Annales Universitatis Apulensis: Series Oeconomica*, *15*(2), 443.

Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud computing and information policy: Computing in a policy cloud? *Journal of Information Technology & Politics*, *5*(3), 269-283.

Jansen, W. A. (2011, January). Cloud hooks: Security and privacy issues in cloud computing. In *2011 44th Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.

Julien, P. A. (1998). Introduction. The state of the art in small business and entrepreneurship. *Ashgate, Aldershote.*, 1.

Kachwanya, K. (2011, November 01). *9 Cloud Computing Challenges you should expect in Kenya*. Retrieved February 14, 2017, from *http://www.kachwanya.com/2011/11/01/7-cloud-computing-challenges-you-should-expect-in-kenya/*

Kavanagh, M. J., & Johnson, R. D. (Eds.). (2017). *Human resource information systems: Basics, applications, and future directions*. Sage Publications.

Keller, E., Szefer, J., Rexford, J., & Lee, R. B. (2010, June). NoHype: Virtualised cloud infrastructure without the virtualisation. *ACM SIGARCH Computer Architecture News, 38*(3), 350-361).

Kenya Gazette Supplement No. 219 (Acts No. 55). (2013) *Kenya Gazette Supplement*.

Kenya Gazette Supplement No. 54 (Acts No. 11). (2017). *Kenya Gazette Supplement*.

Ketel, M. (2008, March). IT security risk management. In *Proceedings of the 46th Annual Southeast Regional Conference on XX* (pp. 373-376). ACM.

Khajeh-Hosseini, A., Greenwood, D., Smith, J. W., & Sommerville, I. (2012). The cloud adoption toolkit: Supporting cloud adoption decisions in the enterprise. *Software: Practice and Experience*, *42*(4), 447-465.

Khalil, I., Khreishah, A., & Azeem, M. (2014). Cloud computing security: A survey. *Computers*, *3*(1), 1-35.

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

Kowalczyk, D. (2015). *Descriptive Research Design: Definition, Examples & Types*. Retrieved from https://study.com/academy/lesson/descriptive-research-design-definition-examples-types.html.

Kuan, K. K., & Chau, P. Y. (2001). A perception-based model for EDI adoption in small businesses using a technology–organisation–environment framework. *Information & Management*, *38*(8), 507-521.

Kumar, R. S., & Saxena, A. (2011, January). Data integrity proofs in cloud storage. In *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)* (pp. 1-4). IEEE.

Lanois, P. (2010). Caught in the clouds: The Web 2.0, cloud computing, and privacy. *Nw. J. Tech. & Intell. Prop.*, *9*, 29.

Letting, N., & Muthoni, M. (2013). Innovation through Business Planning among Micro, Small and Medium Enterprises in Kenya. *Working Paper*. University of Nairobi

Li, Y., & Liu, Z. (2011, August). The ICT industrial interaction between Mainland China and Taiwan: Empirical analysis and policy implications. In *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC)* (pp. 3478-3484). IEEE.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. *NIST special publication*, *500*(2011), 1-28.

Longley, D., Shain, M., & Caelli, W. (1992). *Information security: Dictionary of concepts, standards and terms*. Springer.

Luhmann, N. (2017). *Risk: a sociological theory*. Routledge.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy: An enterprise perspective on risks and compliance*. O'Reilly Media, Inc.

Mathisen, E. (2011, May). Security challenges and solutions in cloud computing. In *5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011)* (pp. 208-212). IEEE.

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

Miller, J. (2000). Risk Management for Your Web Site. *International Risk Management Institute Expert Commentary*.

Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing*, *63*(2), 561-592.

Mohamed, A. (2009, March 01). A history of cloud computing. Retrieved March 12, 2016, from *http://www.computerweekly.com/feature/A-history-of-cloud-computing.*

Mokhtar, S. A., Ali, S. H. S., Al-Sharafi, A., & Aborujilah, A. (2013, January). Cloud computing in academic institutions. In *Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication* (p. 2). ACM.

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

Mukhin, V., & Volokyta, A. (2011, September). Notice of violation of IEEE publication principles security risk analysis for cloud computing systems. In *Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems* (Vol. 2, pp. 737-742). IEEE.

Muthee, J. W. (2016). *A Data Security Implementation Model for Cloud Computing in Government Parastatals*. Published Thesis, University of Nairobi.

Mwobobia, F. M. (2012). The challenges facing small-scale women entrepreneurs: A case of Kenya. *International Journal of Business Administration, 3*(2), 112.

Nassiuma, D. K. (2000). Survey sampling. *Theory and methods.* Nairobi University Press.

National Institute of Standards and Technology. (2017). Retrieved July 24, 2018, from *https://www.nist.gov/*

Omwansa, K. T., Waema, M. T., & Omwenga, B. (2014). Cloud computing in Kenya. *Baseline survey*.

Ongori, H., & Migiro, S. O. (2010). Information and communication technologies adoption in SMEs: Literature review. *Journal of Chinese Entrepreneurship, 2*(1), 93-104.

Oso, Y., & Onen, D. (2011). *Writing research proposal and report*. Nairobi: Jomo Kenyatta Foundation.

Padgett, D. K. (2016). *Qualitative methods in social work research* (Vol. 36). Sage Publications.

Palmer, S. A. (2015). *U.S. Patent No. 9,172,918*. Washington, DC: U.S. Patent and Trademark Office.

Parker, C., & Castleman, T. (2007). New directions for research on SME-eBusiness: Insights from an analysis of journal articles from 2003-2006. *Journal of Information Systems and Small Business*, *1*(1), 21-40.

Parker, D. B. (2012). Toward a new framework for information security? *Computer Security Handbook*, 3-1.

Payne, J. E. (2002). E-commerce readiness for SMEs in developing countries: A guide for development professionals. *Academy for Educational Development/LearnLink*.

Pearson, S. (2013). Privacy, security and trust in cloud computing. In *Privacy and security for cloud computing* (pp. 3-42). Springer, London.

Pearson, S., & Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In *2010 IEEE Second International Conference on Cloud Computing Technology and Science* (pp. 693-702). IEEE.

Peng, Y., & Wang, Y. Z. (2008, December). Research about security audit platform in E-government system. In *2008 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology* (Vol. 3, pp. 235-239). IEEE.

Pierre L., "The Wall Street Networks," (2008). *PITAC, "Cyber-Security: A Crisis of Prioritisation,*" National Coordination Office for Information.

Pleshakova, A. (2018, November 08). 3 Winners & 2 Losers: NIST Cybersecurity Framework 1.1. Retrieved from *https://nehemiahsecurity.com/blog/nist-framework/*

Popović, K., & Hocenski, Ž. (2010, May). Cloud computing security issues and challenges. In *the 33rd International Convention MIPRO* (pp. 344-349). IEEE.

Ramgovind, S., Eloff, M. M., & Smith, E. (2010, August). The management of security in cloud computing. In *2010 Information Security for South Africa* (pp. 1-7). IEEE.

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). A policy framework for information security. *Communications of the ACM, 46*(7), 101-106.

Reveron, D. S. (Ed.). (2012). *Cyberspace and national security: Threats, opportunities, and power in a virtual world*. Georgetown University Press.

Rittinghouse, J. W., & Ransome, J. F. (2016). *Cloud computing: Implementation, management, and security*. CRC press.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121-135.

Rouse, M. (2014). Big data: Big Data and Cloud Business Intelligence. *TechTarget*, 30.

Sallé, M. (2004). IT Service Management and IT Governance: Review, comparative analysis and their impact on utility computing. *Hewlett-Packard Company,* 8-17.

SANS Glossary of Security Terms. (2017). Retrieved May 2018, from https://www.sans.org/security-resources/glossary-of-terms/

Saripalli, P., & Walters, B. (2010, July). Quirc: A quantitative impact and risk assessment framework for cloud security. In *2010 IEEE 3rd International Conference on Cloud Computing* (pp. 280-288). IEEE.

Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report, 15*(3), 112-133.

Seccombe, A., Hutton, A., Meisel, A., Windel, A., Mohammed, A., & Licciardi, A. (2009). Security guidance for critical areas of focus in cloud computing. *Cloud Security Alliance*, *2*(1), 2-70.

Sen, J. (2015). Security and privacy issues in cloud computing. In *Cloud Technology: Concepts, Methodologies, Tools, and Applications* (pp. 1585-1630). IGI Global.

Sen, J., & Sengupta, I. (2005, December). Autonomous agent based distributed fault-tolerant intrusion detection system. In *International Conference on Distributed Computing and Internet Technology* (pp. 125-131). Springer, Berlin, Heidelberg.

Sengupta, S., Kaulgud, V., & Sharma, V. S. (2011, July). Cloud computing security: Trends and research directions. In *2011 IEEE World Congress on Services* (pp. 524-531). IEEE.

Shackelford, S. J., Russell, S., & Haut, J. (2015). Bottoms up: A comparison of voluntary cybersecurity frameworks. *UC Davis Bus. LJ, 16*, 217.

Shroff, G. (2010). *Enterprise cloud computing: Technology, architecture, applications*. Cambridge university press.

Sin Tan, K., Choy Chong, S., Lin, B., & Cyril Eze, U. (2009). Internet-based ICT adoption: Evidence from Malaysian SMEs. *Industrial Management & Data Systems, 109*(2), 224-244.

Srinivasan, G., & Abi-raad, M. (2013). Risk factors associated with e-business infrastructure of SMEs. *Working Paper.* Australian Information Security Management Conference.

Stajano, F., & Anderson, R. (2002). The resurrecting duckling: Security issues for ubiquitous computing. *Computer, 35*(4), supl22-supl26.

Stallings, W., Brown, L., Bauer, M. D., & Bhattacharjee, A. K. (2012). *Computer security: Principles and practice* (pp. 978-0). Upper Saddle River (NJ: Pearson Education.

Sultan, N. (2010). Cloud computing for education: A new dawn? *International Journal of Information Management*, *30*(2), 109-116.

Sultan, N. A. (2011). Reaching for the "cloud": How SMEs can manage. *International Journal of Information Management*, *31*(3), 272-278.

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks*, *10*(7), 190903.

Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, *8*(6), 24-31.

Tan, D. (2002). Quantitative risk analysis step-by-step. *GSEC Practical Version*, *1*.

Technology Dictionary. (2017). Retrieved August 2018, from *https://www.techopedia.com/dictionary*

Tan, F.T. (2010). A perception-based model for technological innovation in small and medium enterprises. In Proceedings of the *European Conference on Information Systems(ECIS), 2010*.

Tim, M., Subra, K., & Shahed, L. (2009). Cloud security and privacy. *O'Reilly Vlg. GmbH & Co.*

Tripathi, A., & Mishra, A. (2011, September). Cloud computing security considerations. In *2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)* (pp. 1-5). IEEE.

Trusted Computing Group. (2010). *Cloud computing and security: A natural match*. Beaverton: Trusted Computing Group.

UAE Chamber of Commerce. (2016). Retrieved from *http://eastafricatop100.com/*

Vahradsky, D. (2012). Cloud risk: 10 principals and a framework for assessment. *ISACA, 5,* 1-12.

Vecchiola, C., Pandey, S., & Buyya, R. (2009, December). High-performance cloud computing: A view of scientific applications. In *2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks* (pp. 4-16). IEEE.

Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. *Information Systems Management*, 24(4), 361-372.

Velte, A. T., Velte, T. J., Elsenpeter, R. C., & Elsenpeter, R. C. (2010). *Cloud computing: A practical approach* (p. 44). New York: McGraw-Hill.

Victories, V. (2015). Types of cloud computing deployment model you need to know. *IBM developer Works. IBM*.

Wahlgren, G., & Kowalski, S. (2013). IT security risk management model for cloud computing: A need for a new escalation approach. *International Journal of E-Entrepreneurship and Innovation (IJEEI)*, *4*(4), 1-19.

Walsham, G., & Sahay, S. (2006). Research on information systems in developing countries: Current landscape and future prospects. *Information Technology for Development*, *12*(1), 7-24.

Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2011). Enabling public auditability and data dynamics for storage security in cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, *22*(5), 847-859.

Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). Toward secure and dependable storage services in cloud computing. *IEEE Transactions on Services Computing*, *5*(2), 220-232.

Wheeler, E. (2011). *Security risk management: Building an information security risk management program from the ground up*. Elsevier.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Williams, M. I. (2010). *A quick start guide to cloud computing: Moving your business into the cloud*. Kogan Page Publishers.

Yeboah-Boateng, E. O. (2013). Fuzzy similarity measures approach in benchmarking taxonomies of threats against SMEs in developing economies. *Canadian Journal on Computing in Mathematics, Natural Sciences, Engineering and Medicine*, *4*(1), 34-44.

Yazar, Z. (2002). A qualitative risk analysis and management tool–CRAMM. *SANS InfoSec Reading Room White Paper*, *11*, 12-32.

Zardari, S., & Bahsoon, R. (2011, May). Cloud adoption: A goal-oriented requirements engineering approach. In *Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing* (pp. 29-35). ACM.

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

Zissis, D., & Lekkas, D. (2012). Is cloud computing finally beginning to mature? *International Journal of Cloud Computing and Services Science, 1*(4), 172.

APPENDICES

APPENDIX I: QUESTIONNAIRES

Dear Sir /Madam,

I am a student pursuing a Doctor of Philosophy in Information Technology Security and Audit at the School of Computer Science, of Kabarak University. I am conducting a Study on "Implementing a Security Framework in Software as a Service (SAAS) Cloud Paradigm for SMEs in Kenya". In this regard, a questionnaire has been developed addressing several aspects related to the subject of Study and I wish to request that you to fill it.

I also wish to assure you that the information hereby given will be used for academic purposes only and will be treated with the utmost confidentiality.

Thank You.

Sincerely,

Mr Satwinder Singh

Kabarak University

SECTION A: PERSONAL DETAILS

Please respond to the questions below by ticking (✓) only 1(one) appropriate option:

1. Gender: Male ( ) Female ( )

2. Indicate your age in the space shown below:

______________________________years

3. What is your level of education?

Indicate your response below by ticking (✓) only 1(one) appropriate option:

Certificate ( ) Tertiary ( ) Degree ( ) Masters ( ) Doctorate ( )

4. How many years have you worked with Information Technology/systems?

Indicate your response below by ticking (✓) only 1(one) appropriate option:

Below 1 year ( ) 1-2 years ( ) 3-4 years ( ) Over 5 years ( )

5. Which of the following best describe your role in the organisation?

Indicate your response below by ticking (✓) only 1(one) appropriate option:

Security Analyst/Administrator ( ) Technician ( )

Other ( ), Specify………………………..

6. How long have you worked in this company?

Indicate your response below by ticking (✓) only 1(one) appropriate option:

Less than a year ( )

Less than two years ( )

Less than three years ( )

Less than four years ( )

7. What services are you hiring or intending to hire from your cloud Service provider?

Please respond to the above question by ticking (✓) only one (1) appropriate option:

ERP ( ) CRM ( ) SAP ( ) Network ( ) Storage ( )

Server ( ) OS ( ) Office suite ( ) Hosted E-mail ( )

Virtual machine instances ( ) Hosted platform ( ) other ( )

SECTION B:

Cloud computing Security issues on SaaS delivery model and their respective deployment models emanates from various security concerns. The following are items that represent security challenges faced in SaaS delivery model in their respective deployment models.

Please respond to the items in each row by ticking only 1 box below the number that closely indicates how you feel.

NB:

5. = Strongly Agree 4 = Agree 3 = Undecided 2 = Disagree 1 = Strongly Disagree

No.	**Item**	**5**	**4**	**3**	**2**	**1**
1	Data/information stored on the cloud may face a lot of availability issues due to downtime in the internet.					
2	A cloud administrator may become a very high risk if they turn rouge and try and access data stored on clouds.					
3	Whenever the data owner makes a command to delete a cloud resource, there is no certain way of telling that the data has been deleted to its entirety.					
4	Because the owner of the data has not control					

	over the data handling practices of the cloud vendor, there is no sure way of telling that data is being handled in a lawful way.					
5	In SaaS model, hackers can manipulate weakness in data security model to get an illegitimate access to data or application.					
6	Cloud computing creates lack of liability of providers in case of security incidents					
7	Multi-tenancy in the cloud a major issue for clients due to the possibility of a hacker taking advantage of the same host					
8	Password protection in itself is enough to secure against unauthorised access in the cloud					

SECTION C:

Areas of Cloud Computing the need to be secured, rate if the cloud provider has sufficient security measures to cater for all the areas.

Please respond to the items in each row by ticking only 1 box below the number that closely indicates how you feel.

NB:

5= Strongly Agree 4 = Agree 3 = Undecided 2 = Disagree 1 = Strongly Disagree

No	**Item**	**5**	**4**	**3**	**2**	**1**
9	Cloud computing supplier maintains proper security monitoring logs of all access to your data and documents access as routine, random audit, or suspicious leveraging their prescribed scripts and operational procedures as the basis for all audit in all deployment models.					
10	User access control rules, security policies and enforcement are made available to the customer in a well-informed manner.					
11	In SaaS, applications are multi-tenant hosted by					

	3rd party usually exposes functionality could result multifaceted security issues					
12	Cloud computing providers provide sufficient security for data at rest. (Stored data in the cloud)					
13	Cloud computing providers provide sufficient security for data in transit. (Data being transferred from the cloud to the user computers and vice versa)					
14	Cloud computing providers provide sufficient authentication platform for users to access the cloud.					
15	Cloud providers have sufficient and credible policies and practices especially for things like data retention, deletion and security.					
16	Customers understand how incidents and disasters will affect their data and therefore have relevant recovery procedures for the same.					

SECTION D:

What are your main concerns in your approach to Cloud Computing?

Please respond to the items in each row by ticking only 1 box below the number that closely indicates how you feel.

NB:

5= Not important 4 = Slightly Important 3 = Undecided 2 = Medium Importance 1 = crucially important

No	**Item**	**5**	**4**	**3**	**2**	**1**
17	Privacy					
18	Availability of services and/or data					
19	Integrity of services and/or data					
20	Confidentiality of corporate data					
21	Loss of control of services and/or data					
23	Lack of liability of providers in case of security					

	incidents					
24	Inconsistency between trans national laws and regulations					
25	Intra-clouds (vendor lock-in) migration					
26	Any other (Please specify)					

APPENDIX II: CLOUD SERVER DEPLOYED

OwnCloud offers customers the software and support to create their own private, on-premises cloud. This allows customers to be in charge of how their data is stored or who may have unauthorised access to their sensitive information. With OwnCloud, a cloud user is able to maintain full control over all confidential documents, knowing exactly where the data is at all times and deciding who may or may not have access to a certain documents and folders.

The official OwnCloud websites provide a good source of documentation on the products. Online forums and other community hosted websites are also useful sources of knowledge, answers can be found to common problems relating to system installations and configurations.

General Recommendations for Installation

- Operating system: Linux.
- Web server: Apache 2.4.
- Database: MySQL/MariaDB with InnoDB storage engine (MyISAM is not supported, see: MySQL / MariaDB storage engine)
- PHP 5.6+.
- Consider setting up a scale-out deployment, or using Federated Cloud Sharing to keep individual OwnCloud instances to a manageable size.

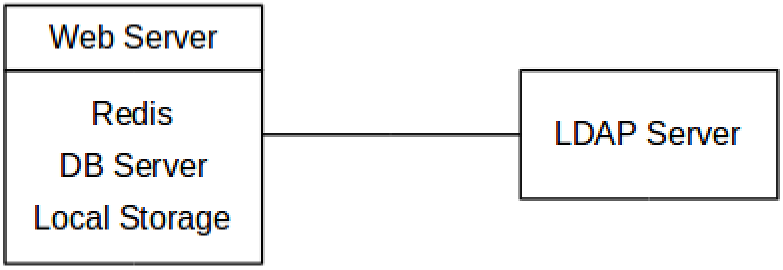
This recommendation applies if you meet the following criteria described below:

Option	Value
Number of users	Up to 150 users
Storage size	100 GB to 10TB
High availability level	Zero-downtime backups via Btrfs snapshots, component failure leads to interruption of service. Alternate backup scheme on other filesystems: nightly backups — with service interruption.

Recommended System Requirements

One machine running the application, web, and database server, as well as local storage.

Authentication via an existing LDAP or Active Directory server.



Components
One server with at least 2 CPU cores, 16GB RAM, and local storage as needed.

Operating system
Enterprise-grade Linux distribution with full support from an operating system vendor. The company recommend both RedHat Enterprise Linux and SUSE Linux Enterprise Server 12.

SSL Configuration
The SSL termination is done in Apache. A standard SSL certificate is required to be installed according to the official Apache documentation.

Load Balancer
None.

APPENDIX III: TOP 100 SMES AS PER NATION BUSINESS DAILY 2016

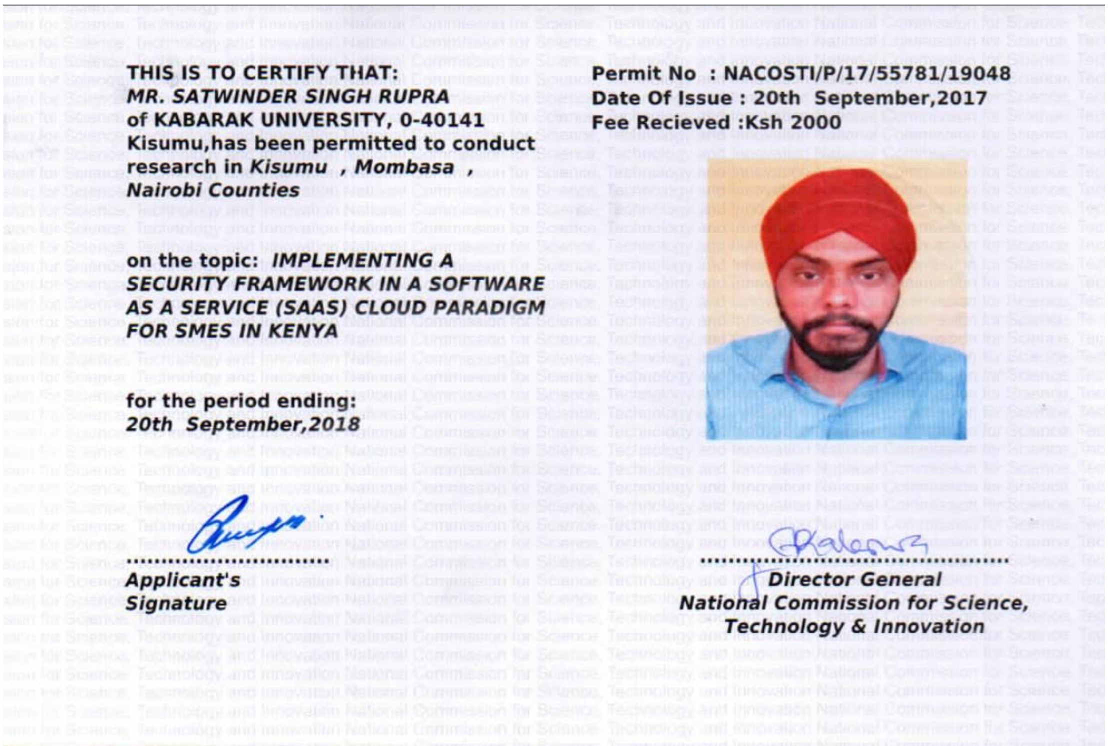
1. Diamond Property Merchants Ltd	Nairobi
2. Izmir Enterprises Limited	Nairobi
3. Soloh Worldwide Enterprises Ltd	Nairobi
4. Advanta Africa Ltd	Nairobi
5. Hipora Business Solutions	Nairobi
6. General Cargo Services Ltd	Nairobi
7. Komal Construction Company Ltd	Nairobi
8. Allwin Packaging Intl Ltd	Nairobi
9. Tangazoletu Limited	Nairobi
10. NorthStar Cooling Systems Ltd	Nairobi
11. Africa Practice EA Ltd	Nairobi
12. Polgon Logistics Limited	Mombasa
13. Manix Ltd	Nairobi
14. Care Chemists	Nairobi
15. Well Told Story	Nairobi
16. Compulynx Limited	Kisumu
17. Aar Credit Service Ltd	Nairobi
18. Coastal Image Technologies Ltd	Mombasa
19. Sheffield Steel Systems Limited	Nairobi
20. Avtech Systems Ltd	Nairobi
21. Polucon Services (K) Ltd	Mombasa
22. Machines Technologies Ltd	Nairobi
23. Orange Pharma Ltd	Nairobi
24. Pindoria Holdings Ltd	Nairobi
25. Computer Pride Limited	Nairobi
26. EDN George EA Limited	Nairobi
27. Valley Hospital Limited	Nakuru
28. Mandhir Construction Ltd	Nairobi
29. Patmat Bookshop Ltd	Nakuru
30. Software Technologies Ltd	Nairobi
31. Trident Plumbers Ltd	Nairobi
32. Superior Homes Kenya Ltd	Nairobi

33. Pathcare Kenya Limited	Kisumu
34. Amex Auto & Ind. Hardware Ltd	Kisumu
35. Rushab Petroleum Limited	Nairobi
36. Phat! Music & Entertainment Ltd	Nairobi
37. Nationwide Electrical Ind. Ltd	Nairobi
38. Unique Offers Ltd	Nairobi
39. Prafulchandra & Brothers Ltd	Nairobi
40. Specicom Technologies Ltd	Nairobi
41. Kisima Drilling (EA) Ltd	Nairobi
42. Executive Healthcare Solutions Ltd	Nairobi
43. Logistics Solutions Ltd	Kisumu
44. Alpha Fine Foods Limited	Nairobi
45. Classic Mouldings Ltd	Nairobi
46. Logistics Link Limited	Nairobi
47. Waterman Drilling Africa Ltd	Nairobi
48. Specialised Aluminium Renovators Ltd	Nairobi
49. Chester Insurance Brokers Ltd	Nairobi
50. Kandia Fresh Produce Suppliers Ltd	Nairobi
51. Sigma Feeds Ltd	Nairobi
52. Kenya Bus Services Mgt.	Nairobi
53. Emmerdale Ltd	Nairobi
54. Mic Global Risks Insurance Brokers Ltd	Nairobi
55. Total Solutions Limited	Nairobi
56. Bluekey Software Solution K Ltd	Nairobi
57. Muranga Forwarders Ltd	Mombasa
58. Impax Business Solutions	Nairobi
59. Warren Concrete Ltd	Nairobi
60. Sensations Ltd	Nairobi
61. Kenbro Industries Ltd	Nairobi
62. Powerpoint Systems EA Ltd	Nairobi
63. Smart Brands Limited	Nairobi
64. Eurocon Tiles Products Ltd	Nairobi
65. Uneek Freight Services Ltd	Nairobi

66. Office Dynamics Limited	Nairobi
67. Jogian Interlink Limited	Nairobi
68. Dataguard Distributors Limited	Nairobi
69. Super-Broom Services Ltd	Nairobi
70. Kencont Logistics Services Ltd	Mombasa
71. Millbrook Garment	Kiambu
72. Palmhouse Dairies Ltd	Nairobi
73. Educate Yourself Limited	Nairobi
74. Orbit Engineering Limited	Nairobi
75. Kisima Electromechanicals Ltd	Nairobi
76. Riley Falcon Security Services Ltd	Kisumu
77. Bagda’s Auto Spares Ltd	Nairobi
78. Vinep Forwarders Limited	Nairobi
79. Economic Industries Limited	Nairobi
80. Fayaz Bakers Limited	Mombasa
81. Spenomatic Kenya Ltd	Nairobi
82. Maroo Polymers Limited	Nairobi
83. Norda Industries Limited	Nairobi
84. Skypex Supplies Limited	Nairobi
85. Master Fabricators Ltd	Nairobi
86. Iron Art Limited	Nairobi
87. Statprint Limited	Nairobi
88. Ideal Manufacturing Co. Ltd	Nairobi
89. Oil Seals and Bearing Centre Ltd	Nairobi
90. Varsani Brakelinings Ltd	Nairobi
91. Synergy Gases (K) Ltd	Mombasa
92. Rift Valley Machinery Services	Kisumu
93. De Ruiter East Africa Limited	Nairobi
94. Newline Ltd	Nairobi
95. R&R Plastics Limited	Nairobi
96. Vivek Investments Ltd	Nairobi
97. Ndugu Transport Company Ltd	Kisumu
98. Circuit Business System Ltd	Nairobi

99. Thika Cloth Mills Ltd	Nairobi
100. Hotel Waterbuck Ltd	Nakuru

APPENDIX IV: RESEARCH LICENCE



THIS IS TO CERTIFY THAT:
MR. SATWINDER SINGH RUPRA
of KABARAK UNIVERSITY, 0-40141
Kisumu,has been permitted to conduct research in *Kisumu , Mombasa , Nairobi Counties*

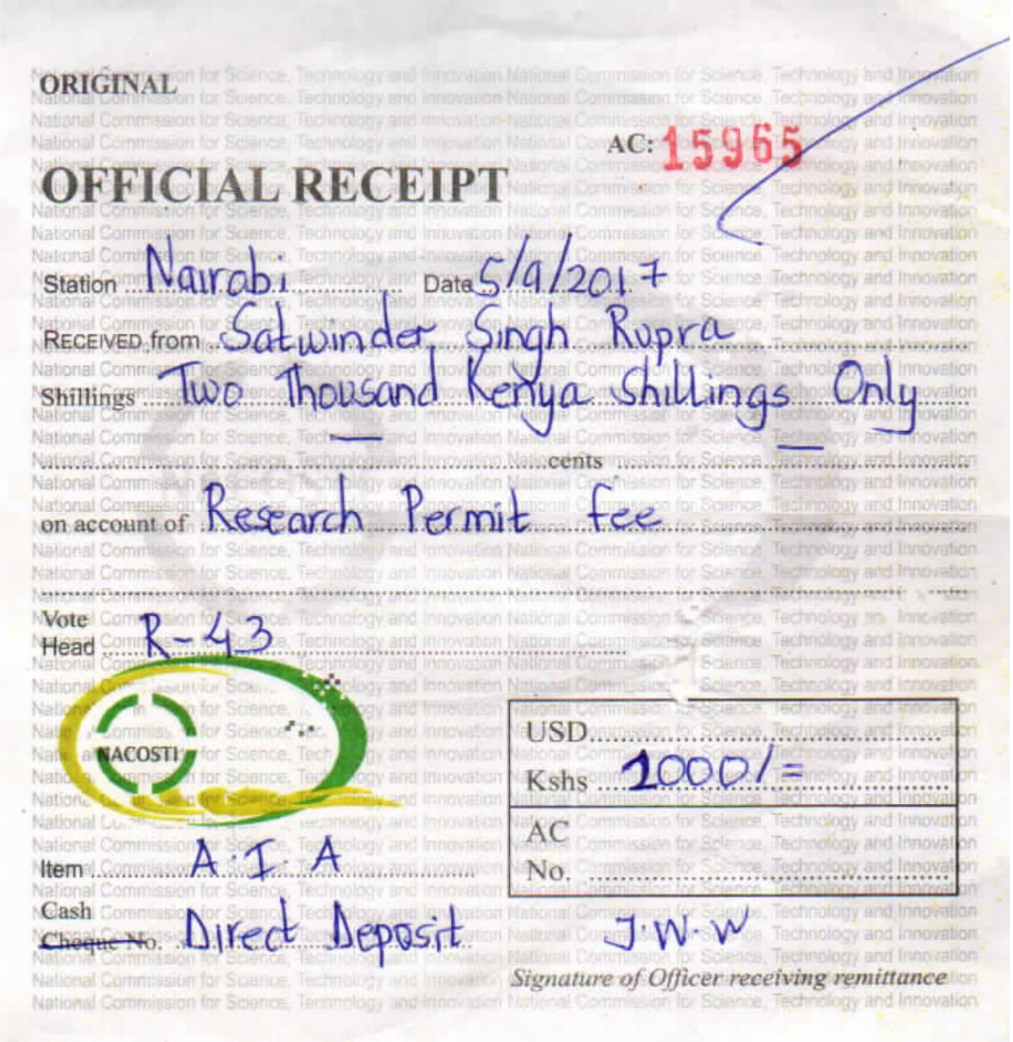
on the topic: *IMPLEMENTING A SECURITY FRAMEWORK IN A SOFTWARE AS A SERVICE (SAAS) CLOUD PARADIGM FOR SMES IN KENYA*

for the period ending:
20th September,2018

Permit No : NACOSTI/P/17/55781/19048
Date Of Issue : 20th September,2017
Fee Recieved :Ksh 2000

Applicant's Signature

Director General
National Commission for Science, Technology & Innovation



ORIGINAL

AC: 15965

OFFICIAL RECEIPT

Station Nairobi Date 5/9/2017

RECEIVED from Satwinder Singh Rupra

Shillings Two Thousand Kenya Shillings Only

cents

on account of Research Permit fee

Vote Head R-43

NACOSTI

USD

Kshs 2000/=

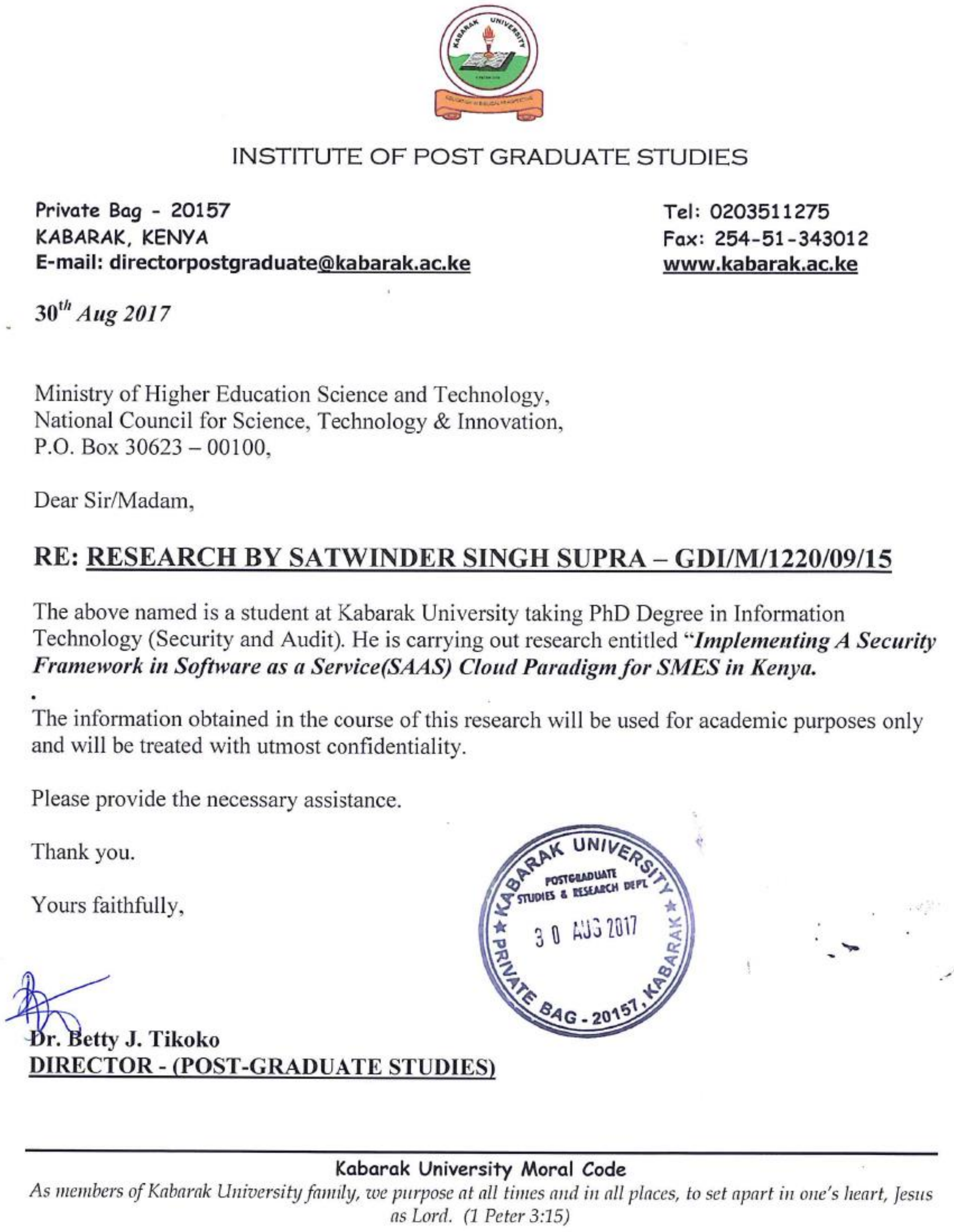
AC No.

Item A I A

Cash ~~Cheque No.~~ Direct Deposit

J.W.W

Signature of Officer receiving remittance



INSTITUTE OF POST GRADUATE STUDIES

Private Bag - 20157
KABARAK, KENYA
E-mail: directorpostgraduate@kabarak.ac.ke

Tel: 0203511275
Fax: 254-51-343012
www.kabarak.ac.ke

30th Aug 2017

Ministry of Higher Education Science and Technology,
National Council for Science, Technology & Innovation,
P.O. Box 30623 – 00100,

Dear Sir/Madam,

RE: RESEARCH BY SATWINDER SINGH SUPRA – GDI/M/1220/09/15

The above named is a student at Kabarak University taking PhD Degree in Information Technology (Security and Audit). He is carrying out research entitled "***Implementing A Security Framework in Software as a Service(SAAS) Cloud Paradigm for SMES in Kenya.***

The information obtained in the course of this research will be used for academic purposes only and will be treated with utmost confidentiality.

Please provide the necessary assistance.

Thank you.

Yours faithfully,

Dr. Betty J. Tikoko
DIRECTOR - (POST-GRADUATE STUDIES)

KABARAK UNIVERSITY
POSTGRADUATE STUDIES & RESEARCH DEPT
30 AUG 2017
PRIVATE BAG - 20157, KABARAK

Kabarak University Moral Code

As members of Kabarak University family, we purpose at all times and in all places, to set apart in one's heart, Jesus as Lord. (1 Peter 3:15)